

BLOCKBIT UTM

SWG – Secure

Web Gateway

Proxy Web Filter

Versão 2.2

Release 2



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.

Edição: Setembro/2022

Autor: Nemias Tavares Jr (NTJr.)

Fale com nossos especialistas.

Contatos:

AMERICA DO NORTE (Sede)

703 WaterFord Way – 4th floor

Miami – FL – 33126

UNITED STATES

Tel: +1 305 373 4660

EUROPA (Escritório Principal)

2 Kingdom Street – 6th floor

Paddington – London – W2 6J P

UNITED KINGDOM

Tel: +44 203 580 4321

AMÉRICA LATINA (Escritório Principal)

R. Alexandre Dumas, 1711- Edifício Birmann 11 – Térreo

Chácara Santo Antônio

São Paulo – SP – 04717-911

BRASIL

Tel: +55 11 2165 8888

Email: support@blockbit.com

Site: www.blockbit.com

APRESENTAÇÃO

Obrigado por escolher as soluções de segurança Blockbit Platform It's easy to be secure.

Com mais de 20 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 Inteligente Lab que trabalha 24x7x365 na pesquisa e análise de novas ameaças melhorando a segurança de sua empresa.

O Blockbit UTM Network Security 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

| | |
|--|-----------|
| 1. INTRODUÇÃO | 7 |
| 1.1. Estrutura do Treinamento | 7 |
| 2 PROXY | 8 |
| 3.1 Proxy HTTP | 10 |
| 3.2 Proxy FTP..... | 13 |
| 3.3 Proxy SMTP | 14 |
| 3.4 Proxy POP..... | 15 |
| 3.5 Inspeção SSL..... | 19 |
| 3.5.1 Perfil Inspeção SSL 1 - Protocolo HTTPs..... | 21 |
| 3.5.2 Perfil Inspeção SSL 2 – Protocolo SMTPs..... | 22 |
| 3.5.3 Perfil de Inspeção SSL 3 – Protocolo POP3s..... | 23 |
| 3.6 Exceção de Inspeção SSL..... | 24 |
| 3.6.1 Exceção Inspeção SSL 1 – Web Categorias de exceção | 25 |
| 4 WEB CACHE | 27 |
| 5 WEB FILTER | 32 |
| 7.1 Configurações Web Filter | 35 |
| 7.2 Perfis Web Filter | 37 |
| 7.3 Entendendo a criação dos Perfis Web Filter..... | 40 |

| | | |
|-------|--|----|
| 7.3.1 | <i>Perfil Web Filter 1 – Navegação Inapropriada</i> | 41 |
| 7.3.2 | <i>Perfil Web Filter 2 – Navegação Segura</i> | 48 |
| 7.3.3 | <i>Perfil Web Filter 3 – Controle G Suite Google</i> | 53 |
| 7.3.4 | <i>Perfil Web Filter 4 – Navegação Wi-Fi Corp – [Surf Control]</i> | 57 |
| 7.3.5 | <i>Perfil Web Filter 5 – Navegação Rede Wi-Fi [Safe Browsing]</i> | 62 |

1. Introdução

O Treinamento Oficial Blockbit UTM tem como objetivo a capacitação do profissional de rede para que obtenha o domínio completo da ferramenta incluindo técnicas de diagnóstico (troubleshooting), cenários de uso e situações do dia a dia em ambientes de rede de diversos tamanhos e aplicações.

1.1. Estrutura do Treinamento

O Treinamento Oficial Blockbit UTM está organizado da seguinte forma:

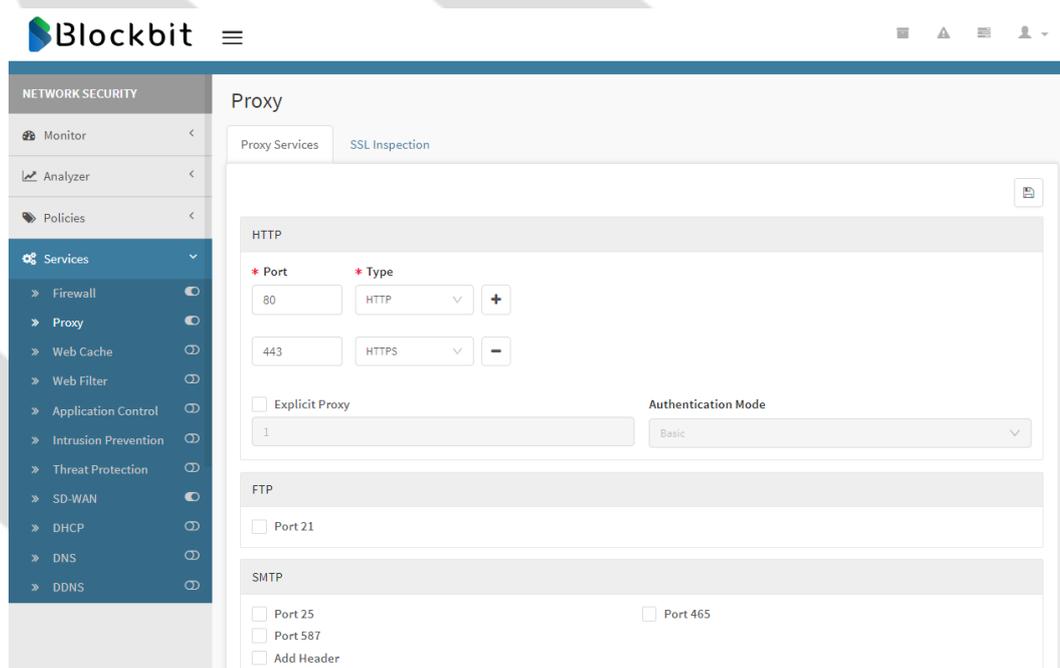
- Introdução / Conceitos
- Preparação do ambiente / Instalação Inicial
- Conteúdo técnico / Exercícios

2 Proxy

Vamos abordar os aspectos de segurança da rede por meio da interceptação de “Proxies”.

Os “proxies” são sistemas ou aplicações que atuam como intermediários para as requisições clientes que solicitam recursos de outros servidores. Uma aplicação cliente conecta-se a um servidor “proxy”, solicitando algum serviço, ex.: “uma conexão”, “uma página web”, “um arquivo”, ou “outros recursos” de outros servidores. O Proxy repassa esta requisição para o servidor remoto (normalmente na rede pública), e devolve sua resposta para o cliente interno (host da rede local).

Para configuração e habilitação dos serviços de Proxy, clique em [Services] >> [Proxy].



Recomenda-se: A habilitação do serviço [ / ] antes da sua configuração.

Na maioria das vezes os proxies são utilizados por todos os clientes de uma sub-rede e devido a sua posição estratégica, normalmente eles implementam um sistema de cache para alguns serviços. Além disso, como os proxies trabalham com dados das aplicações, para cada serviço é necessário um proxy diferente.

O Blockbit UTM, inclui serviços de segurança por meio de proxies ativos.

Protocolos e serviços suportados

- HTTP.
- FTP.
- SMTP.
- POP

3.1 Proxy HTTP

O recurso Proxy HTTP é fornecido integrado pelo serviço Web Cache que consiste em oferecer como principal recurso, entre as suas diversas funcionalidades, o acesso à Internet para usuários de uma rede ou 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”, e ao serviço de “AntiMalware” para filtros de arquivos comprometidos, através das políticas de segurança que restringem a navegação dos usuários.

Porta padrão do Proxy: [Porta 128].

Modos de Operação:

[Transparente]

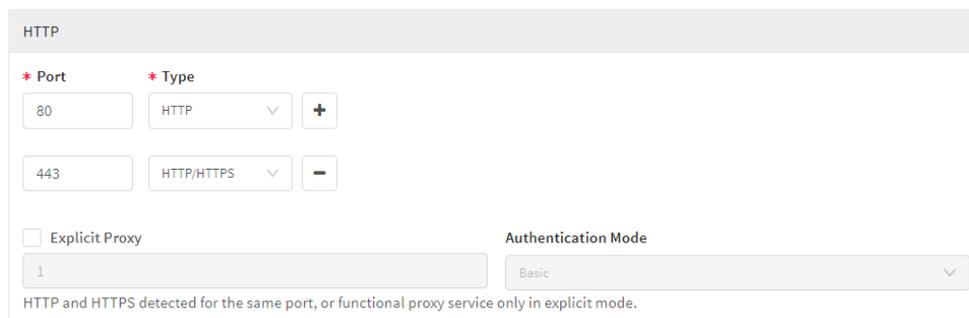
Neste modo de operação o proxy é configurado para permitir o tráfego Http/Https, o gerenciamento e controle do tráfego Https sob a interceptação SSL, exige a importação e instalação do CA (Certification Authority) para todos os dispositivos da rede.

[Explícito]

Para acesso ao proxy no modo explícito é necessário configurar o navegador WEB dos dispositivos da rede para acesso ao proxy no modo configurado.

(Verificar itens de configuração de proxy de cada navegador respectivamente).

No quadro [HTTP] você configura as portas suportadas pelo proxy web Http.



| * Port | * Type |
|--------|------------|
| 80 | HTTP |
| 443 | HTTP/HTTPS |

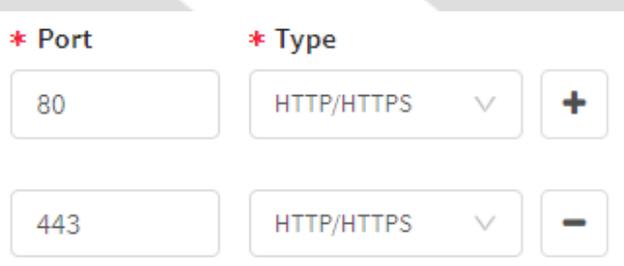
Explicit Proxy

Authentication Mode: Basic

HTTP and HTTPS detected for the same port, or functional proxy service only in explicit mode.

O serviço é pré-configurado para permitir acesso aos serviços web padrões “HTTP (porta 80) e HTTPS (porta 443)”. As portas de serviços são configuráveis com suporte aos protocolos “HTTP e HTTPS versões 1.0 e 1.1”.

A Opção de protocolo no modo “Merge” [HTTP/ HTTPS] como ilustrada na imagem abaixo:



| * Port | * Type |
|--------|------------|
| 80 | HTTP/HTTPS |
| 443 | HTTP/HTTPS |

Restringe o funcionamento do “Proxy” no modo “Explícito”, ignorando todas as políticas de segurança para o proxy no modo “Transparente”

[] Explicit Proxy

[HTTP and HTTPS detected for the same port, or functional proxy service only in explicit mode.]

Habilita de maneira exclusiva o modo funcional do proxy para o modo “Explícito”.

[Authentication Mode]

Seleção do modo de autenticação proxy para o modo explícito.

A habilitação do modo “Explícito” requer a seleção do modo de autenticação como requisito obrigatório.

- [Basic] O esquema de autenticação “Basic” HTTP é definido pela RFC 7617, transmitindo credenciais como pares de ID/senhas de usuários, codificadas usando base64. O Blockbit UTM adiciona os protocolos “HTTPs/ TLS” ao método “Basic” como aprimoramento e segurança adicional.
- [Captive portal] O esquema de autenticação “Captive portal” utiliza o recurso do “Portal de autenticação WEB”, esse método funciona como um serviço de “Redirecionamento automático” de autenticação.

O usuário ao digitar o endereço de qualquer site no navegador, sua requisição é interceptada pelo sistema e é redirecionado para o “Portal de autenticação Web” que solicita a autenticação,

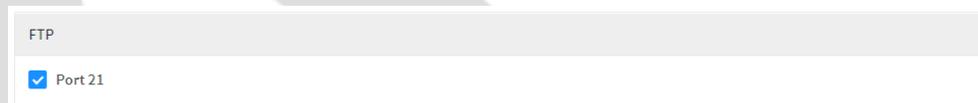
Para habilitação do serviço “Proxy service Http” clique em Save [].

3.2 Proxy FTP

Nesta seção vamos abordar o serviço de Proxy FTP, uma aplicação integrada ao Blockbit UTM com a finalidade de inspecionar o tráfego de transferência de arquivos entre as redes locais e a rede pública (Internet) sob o protocolo FTP de modo seguro.

A sua função básica é possibilitar ao administrador através das “Políticas de segurança” o tratamento dos pacotes e transferências de arquivos por meio do tráfego das portas FTP “20 e 21/TCP” com a interceptação do proxy com suporte a “Scan de vírus e malware”, no modo transparente.

Clique em [Services] >> [Proxy] aba [Proxy Services] acesse o quadro [FTP]



[•] Port 21

Habilitação da porta de conexão com os servidores FTP Remotos. Porta [21/TCP].



O redirecionamento dos arquivos do tráfego FTP para inspeção [Malware Scanning], requer “Políticas de segurança” integradas com o serviço “Threat Protection”.

O recurso de inspeção Threat Protection requer a configuração de um “Perfil”.

- Modo de operação: [FTP Ativo].



TODOS OS ARQUIVOS identificados como “Infectados” pelo serviço Threat Protection via tráfego FTP PROXY são DESCARTADOS.

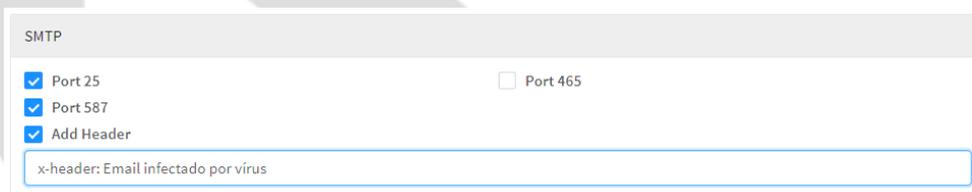
Para habilitação do serviço “Proxy service Ftp” clique em Save [].

3.3 Proxy SMTP

Nesta seção vamos abordar o serviço de Proxy SMTP, uma aplicação integrada ao Blockbit UTM com a finalidade de inspecionar o tráfego de Emails entre “Cliente-Servidor” e “Servidor-Servidor” sob o protocolo SMTP de modo seguro.

A sua função básica é possibilitar ao administrador através das “Políticas de segurança” o tratamento dos pacotes e transferências de arquivos por meio do tráfego das portas SMTP, “[25, 465, 587/TCP]”, com a interceptação do proxy com suporte a “Scan de vírus e malware”, no modo transparente.

Clique em [Services] >> [Proxy] aba [Proxy Services] acesse o quadro [SMTP]



SMTP

Port 25 Port 465

Port 587

Add Header

x-header: Email infectado por virus

[•] Port 25

Habilitação da porta padrão de conexão com os servidores SMTP Remotos. Porta [SMTP - 25/TCP]. {Conexões da porta SMTP 25 normalmente se aplica a conexões entre servidores SMTP.}.

[•] Port 587

Habilitação da porta SMTP Submission de conexão com os servidores SMTP Remotos. Porta [SMTP Sub 587/TCP].



É recomendável o uso da porta 587 nas conexões cliente-servidor.

O Tráfego SMTP Submission exige a autenticação cliente-servidor no protocolo SMTP, o que dificulta o uso indevido de contas de email ou de estações máquinas “zumbis”, método bastante utilizado por spammers.

[•] Add Header

Add Header

x-header: Email infectado com vírus

Este campo contempla um recurso de “Sinalização” que devolve ao usuário um conteúdo “Informativo” quanto ao tratamento aplicado sobre o Email enviado no cabeçalho do respectivo Email. Ex.: “x-header: Email Infectado com vírus.”.

[•] Port 465

Habilitação da porta SMTPS de conexão com os servidores SMTP over SSL/TLS Remotos. Porta [SMTPS - 465/TCP]. {O tráfego SSL/ TLS cliente-servidor exige que a origem possua um certificado digital que seja conhecido pelo servidor SMTP remoto.}



O redirecionamento dos arquivos do tráfego SMTP para inspeção [Malware Scanning], requer “Políticas de segurança” integradas com o serviço “Threat Protection”.

O recurso de inspeção Threat Protection requer a configuração de um “Perfil”.



TODOS OS ARQUIVOS identificados como “Infectados” pelo serviço Threat Protection via tráfego SMTP PROXY são **DESCARTADOS**.

Para habilitação do serviço “Proxy service SMTP” clique em Save [].

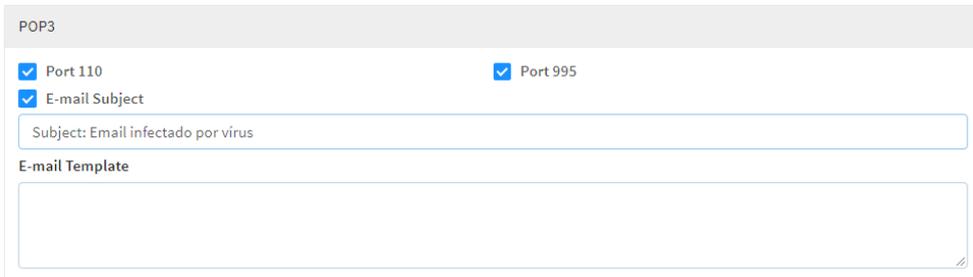
3.4 Proxy POP

Nesta seção vamos abordar o serviço de Proxy POP, uma aplicação integrada ao Blockbit UTM com a finalidade de inspecionar o tráfego de Emails entre “Cliente-Servidor” sob o protocolo POP de modo seguro.

A sua função básica é possibilitar ao administrador através das “Políticas de segurança” o tratamento dos pacotes e transferências de arquivos por meio do

tráfego das portas POP, “[110, 995/TCP]”, com a interceptação de um proxy com suporte a “Scan de vírus e malware”, no modo transparente.

Clique em [Services] >> [Proxy] aba [Proxy Services] acesse o quadro [POP]



[•] Port 110

Habilitação da porta padrão de conexão com os servidores POP Remotos. Porta [POP3 - 110/TCP].

[•] Port 995

Habilitação da porta POP3S de conexão com os servidores POP3 over SSL/TLS Remotos. Porta [POP3S - 995/TCP].



É recomendável o uso da porta 995 nas conexões cliente-servidor.

O Tráfego POP3S aumenta a segurança no tráfego POP3 cliente-servidor. O tráfego SSL/TLS, exige que a origem possua um certificado digital que seja conhecido pelo servidor POP remoto.}.

[•] Email Subject

Email Subject

Subject: Email Infectado por vírus...

Este campo contempla um recurso de “Sinalização” que devolve ao usuário um Email de notificação do tipo “Mailer Postmaster” Informativo quanto ao tratamento aplicado sobre o Email recebido pelo proxy POP do servidor POP remoto.

Email Template

Este campo contempla o “Conteúdo do corpo” do Email de notificação “enviado” para a caixa postal local do usuário final para cada email identificado como “Infectado”. Os valores dos campos em destaque abaixo correspondem aos dados de variáveis retornados pelo tratamento do “Antimalware”.

* E-mail Template

```
Hello !
This message body was generated automatically from Blockbit UTM, wich scanning all incoming email.
It replaces the body of a messages sent to you that contained a VIRUS!
Instead of the infected email this message has been sent to you.
You may look at the message header of this message for the complete email header Information of the infected message.

Virus name:
  %VIRUSNAME%
(Supposed) Sender of the email:
  %MAILFROM%
Sent To:
  %MAILTO%
On Date:
  %MAILDATE%
Subject:
  %SUBJECT%
Connection data:
  %PROTOCOL%from%CLIENTIP%:%CLIENTPORT%toSERVERIP%:%SERVERPORT%
```

Modelo de texto sugerido para uso no template.

Hello !
This message body was generated automatically from Blockbit UTM. wich scanning all incoming email.
It replaces the body of a messages sent to you that contained a VIRUS!
Instead of the infected email this message has been sent to you.
You may look at the message header of this message for the complete email header Information of the infected message.

Virus name:
%VIRUSNAME%
(Supposed) Sender of the email:
%MAILFROM%
Sent To:
%MAILTO%
On Date:
%MAILDATE%
Subject:
%SUBJECT%
Connection data:
%PROTOCOL%from%CLIENTIP%:%CLIENTPORT%toSERVERIP%:%SERVERPORT%
%



O redirecionamento dos arquivos do tráfego POP3 para inspeção [Malware Scanning], requer “Políticas de segurança” integradas com o serviço “Threat Protection”.

O recurso de inspeção Threat Protection requer a configuração de um “Perfil”.



TODOS OS ARQUIVOS identificados como “Infectados” pelo serviço Threat Protection via tráfego Proxy POP são DESCARTADOS.

Para habilitação do serviço “Proxy service POP3” clique em Save [].

3.5 Inspeção SSL

A maioria das informações que trafegam na web usam conexões criptografadas. O Blockbit UTM conta com decriptografia SSL para inspeção de tráfego, garantindo o controle total e o gerenciamento no acesso e aplicando recursos avançados, como : Filtro de conteúdo, ATP, IPS, APP Control e AntiMalware.

A interceptação SSL permite inspecionar os sites e aplicações em HTTP/s que antes passavam pelo sistema em forma de túnel criptografado. Em uma pesquisa realizada pela NSS LABS foi identificado que 72% dos acessos dos serviços WEB trafegam através desse protocolo. A interceptação do SSL permite um maior controle dos acessos dos usuários principalmente em serviços da WEB 2.0. Hoje é praticamente indispensável esse recurso em firewalls.

O Blockbit UTM permite fazer essa interceptação através de “*Perfis SSL Inspection*” às políticas integradas a um serviço de proxy, ou seja, só é efetuada a interceptação para o tráfego que o administrador desejar, desde uma categoria, um site ou outra condição em que a política se aplique.

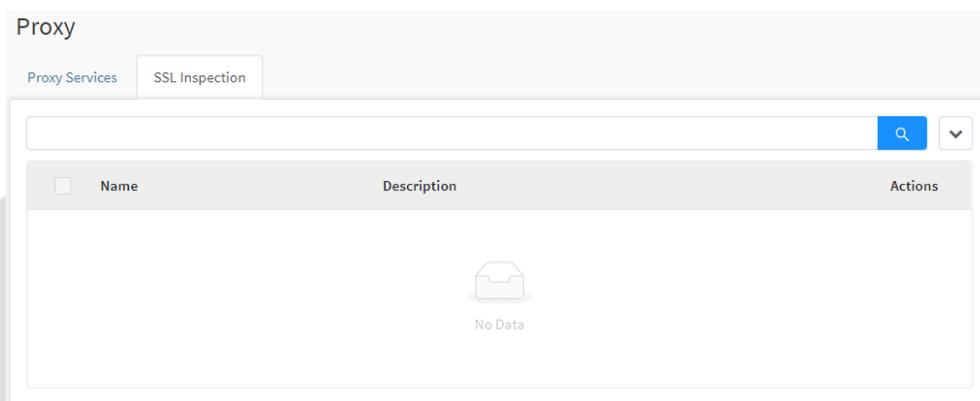
Muitos vírus/malwares previamente instalados em computadores passam pelas políticas de segurança das empresas através das portas SSL como é o caso da porta 443 sem que qualquer antivírus consiga fazer suas análises, com a interceptação SSL o Threat Blocking do Blockbit UTM realiza essa análise, detecta e bloqueia o tráfego do pacote, com base nos perfis e nas compliances das políticas de segurança aplicadas no sistema.

Para a interceptação SSL é necessário criar um C.A. (Certificado de Autoridade) no gateway e exportar para todos os dispositivos da rede (estações de trabalho (PC), mobiles, notebooks, palms e tablets). Esse C.A. é criado automaticamente no Wizard de instalação do Blockbit UTM.

Protocolos suportados

- HTTPs
- SMTPs
- POP3s

Clique na aba [SSL Inspection]



Os Perfis para “Inspeção SSL” se aplicam nas “Políticas de Segurança” integradas aos serviços de segurança “Proxy Web Filter, IPS, APP Control, e Threat Protection”.

Vamos exemplificar a criação de “Perfis de inspeção SSL” para cada modelo de protocolo suportado. Para depois aplicarmos ao modelo de políticas de Proxy – SWG.



Cada “Perfil de inspeção SSL” requer a especificação do número de “Núcleos de Processos Simultâneos” no carregamento para aquele perfil. Cada processo refere-se a um núcleo de processador ou número de filas de processamento ou threads. Seu valor deve ser “≤ menor ou Igual” ao número de núcleos de processamento disponíveis do seu Appliance. {Requisito Obrigatório}.

3.5.1 Perfil Inspeção SSL 1 - Protocolo HTTPs

Adicionar um perfil de inspeção SSL. Clique em Create Profile [] e configure de acordo com as definições para os filtros que deseja aplicar para o protocolo suportado *HTTPs*, habilitar um “01 Núcleo de Processors” e bloquear “Certificados Inválidos”. Depois clique em [Save].

| | |
|-------------|---|
| Name | SSL Inspection HTTPs |
| Description | SSL Inspection HTTPs |
| Workers | Especifique: N° de Núcleos de Processamento: [1] |
| Protocols | Selecione: [<input checked="" type="checkbox"/>] HTTPs |
| Mask | Selecione: [<input checked="" type="checkbox"/>] Block invalid certificates |
| Exception | <i>Null</i> |

3.5.2 Perfil Inspeção SSL 2 – Protocolo SMTPs

Adicionar um perfil de inspeção SSL. Clique em Create Profile [] e configure de acordo com as definições para os filtros que deseja aplicar para o protocolo suportado SMTPs, habilitar um “01 Núcleo de Processors” e bloquear “Certificados Inválidos”. Depois clique em [Save].

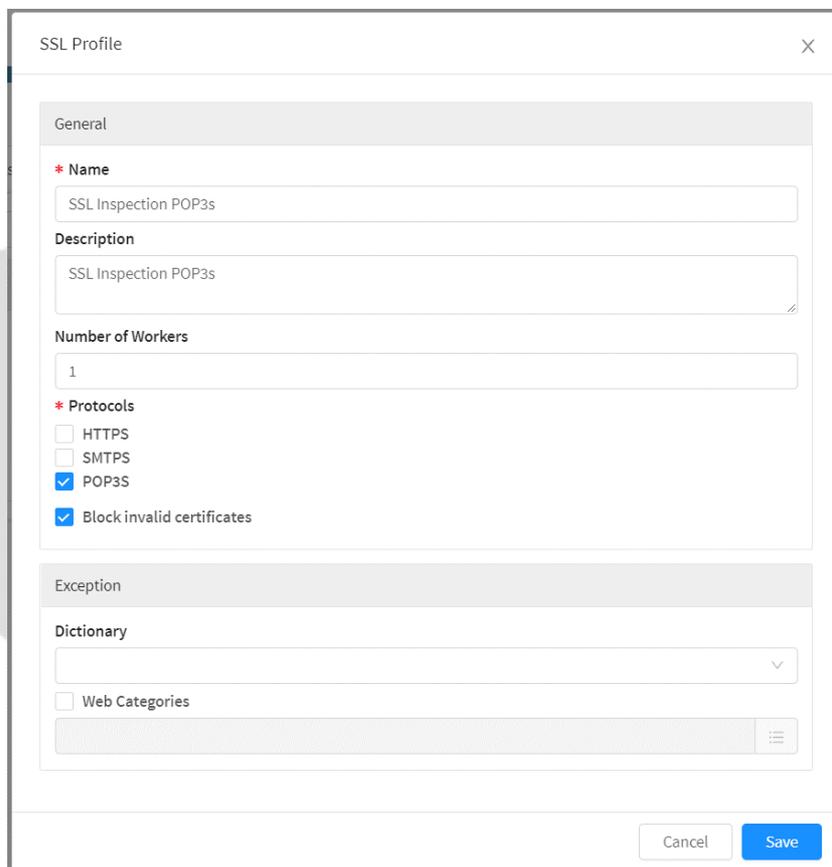
| | |
|-------------|---|
| Name | SSL Inspection SMTPs |
| Description | SSL Inspection SMTPs |
| Workers | Especifique: N° de Núcleos de Processamento: [1] |
| Protocols | Selecione: [<input checked="" type="checkbox"/>] SMTPs |
| Mask | Selecione: [<input checked="" type="checkbox"/>] Block invalid certificates |
| Exception | Null |

3.5.3 Perfil de Inspeção SSL 3 – Protocolo POP3s

Adicionar um perfil de inspeção SSL. Clique em Create Profile [] e configure de acordo com as definições para os filtros que deseja aplicar para o protocolo suportado POP3s, habilitar um “01 Núcleo de Processors” e bloquear “Certificados Inválidos”. Depois clique em [Save].

| | |
|-------------|--|
| Name | SSL Inspection POP3s |
| Description | SSL Inspection POP3s |
| Workers | Especifique: N° de Núcleos de Processamento: [1] |
| Protocols | Selecione: [<input checked="" type="checkbox"/>] POP3s |

| | |
|-----------|---|
| Mask | Selecione: [√] Block invalid certificates |
| Exception | Null |



3.6 Exceção de Inspeção SSL

Existem alguns contratempos da interceptação SSL que devemos conviver.

O correto é que todas as aplicações que utilizam do protocolo SSL tenham acesso aos certificados do sistema ou do navegador, mais algumas aplicações, por questões de segurança, ou mau implementadas ou maliciosas, não suportam esse recurso e acabam sendo abortadas. Alguns exemplos:

- Aplicações do governo.
- Sites de Instituições financeiras
- Skype

Nos dois primeiros casos a aplicação não lê os certificados do sistema e também não tem a opção de importar o certificado em sua aplicação.

No terceiro caso, o Skype é um aplicativo mal-intencionado e não permite fazer a interceptação e por isso também não lê certificados externos.

Nesses casos é necessário permitir o tráfego no modo “by-pass” para essas aplicações, seja via “NAT” ou com a criação de “Perfis de inspeção SSL com listas de exceção” por “Palavras chaves/ Expressões regulares” ou “Categorias Web” para esses serviços.

Defina perfis de exceções para inspeção SSL para destinos confiáveis que pretende permitir o acesso em conformidade com a política corporativa. Alguns conteúdos criptografado que passam pelo gateway não podem ser inspecionados, como alguns exemplos já citados e, portanto, podem ser ignorados com uma única definição de compliance por meio das políticas de segurança, pelo administrador.

Você pode optar por filtrar o tráfego HTTPS sem inspeção SSL.

Vamos exemplificar a criação de “Perfis de exceção na inspeção SSL”.

3.6.1 Exceção Inspeção SSL 1 – Web Categorias de exceção

Clique em Create Profile [] e configure de acordo com as definições para os filtros que deseja aplicar exceção “Web Categories” para o protocolo HTTPs. Depois clique em [Save].

Para definir esta lista de categorias é interessante consultar antes a base de categorias web em: [Monitor] >> [Diagnostics] na aba [Category Lookup], ou na própria interface [Create Profile] quadro [Exception] > [Web Categories] ... [≡]].

Exemplo de lista de algumas categorias para exceção à inspeção SSL.

| Categories | |
|------------------------------|-----------------------|
| Business and Economy (* all) | New and Media (* all) |
| Education (* all) | Religion (* all) |

| | |
|-----------------------|------------------------------|
| Government (*all) | Shopping (*all) |
| URL Translation Sites | Social Organizations (* all) |
| | |

Configure de acordo os campos de configuração do perfil, como segue: “SSL Inspection HTTPs - Exception Categories”

| | |
|-------------|--|
| Name | SSL Inspection HTTPs - Exception Categories |
| Description | SSL Inspection HTTPs - Exception Categories |
| Workers | Especifique: Nº de Núcleos de Processamento: [1] |
| Protocols | Selecione: [<input checked="" type="checkbox"/>] HTTPs |
| Mask | Selecione: [<input type="checkbox"/>] Block invalid certificates |
| Exception | Selecione: Web Categories [☰]. {Listadas acima} |

SSL Profile
✕

General

*** Name**

Description

Number of Workers

*** Protocols**

HTTPS

SMTPS

POP3S

Block invalid certificates

Exception

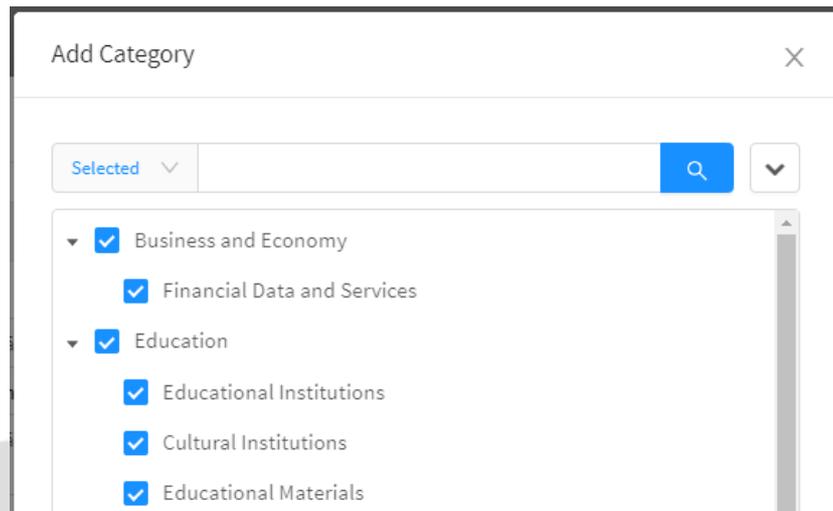
Dictionary

Web Categories

23 Selected
☰

Cancel Save

[☰].



NÃO se esqueça de APLICAR A Fila de comandos []

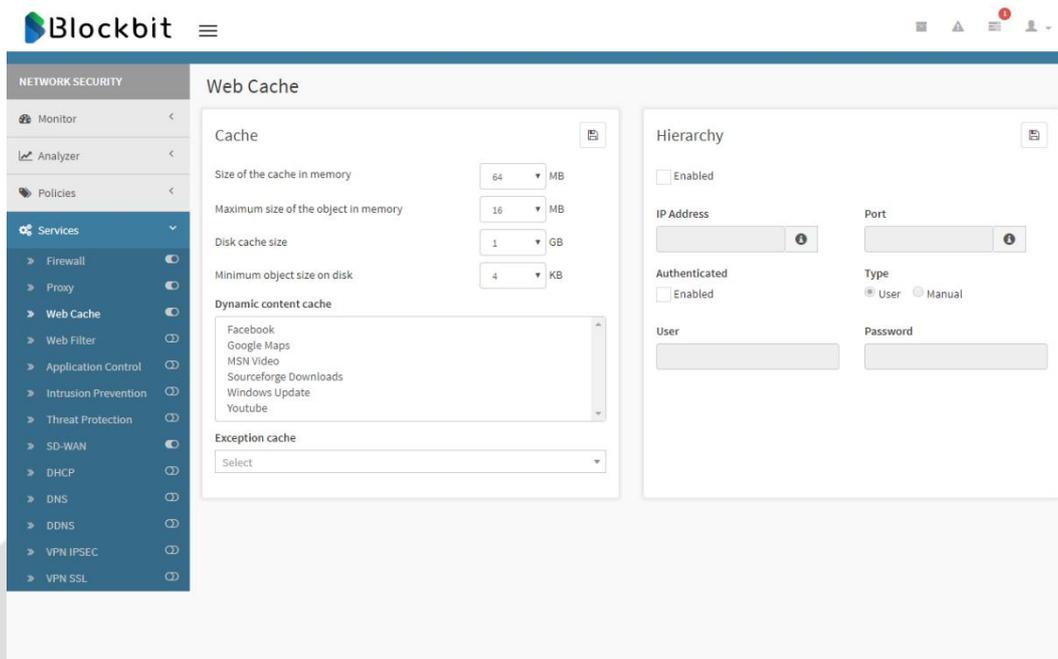
4 Web Cache

O mecanismo de “Web Cache” consiste em minimizar os custos de acesso à Web, reduzir a latência neste tipo de acesso é uma questão muito importante, ainda mais quando considera-se que 3/4 do tráfego de internet atual é gerado nos acessos web (Http/ Https).

O sistema de cache armazena localmente objetos (páginas HTML's, imagens e arquivos) da internet, esse recurso melhora significadamente a qualidade do serviço oferecido aos usuários.

A configuração do serviço Web Cache é definida pela configuração dos controles de cache e ainda conta com o recurso de redirecionamento do tráfego para um proxy hierárquico.

Para acesso a configuração do Web Cache, clique em [Services] >> [Web Cache]



Recomenda-se: A habilitação do serviço [ / ] antes da sua configuração.

[Cache]

No quadro [Cache] temos os 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 reaproveitar o acesso a esses documentos sem que haja a necessidade de estabelecer uma nova conexão com o servidor remoto.

Configuração da cache em memória e disco.

Tamanho máximo e mínimo dos arquivos referentes aos acessos Web que serão salvos/carregados em memória quando do 1º (primeiro) acesso para entrega imediata aos usuários quando requisitados novamente.

- Size of the cache in memory
- Maximum size of the Object in memory
- Disk cache size
- Minimum Object size on disk

Cache de conteúdos dinâmicos. [Dynamic content cache]

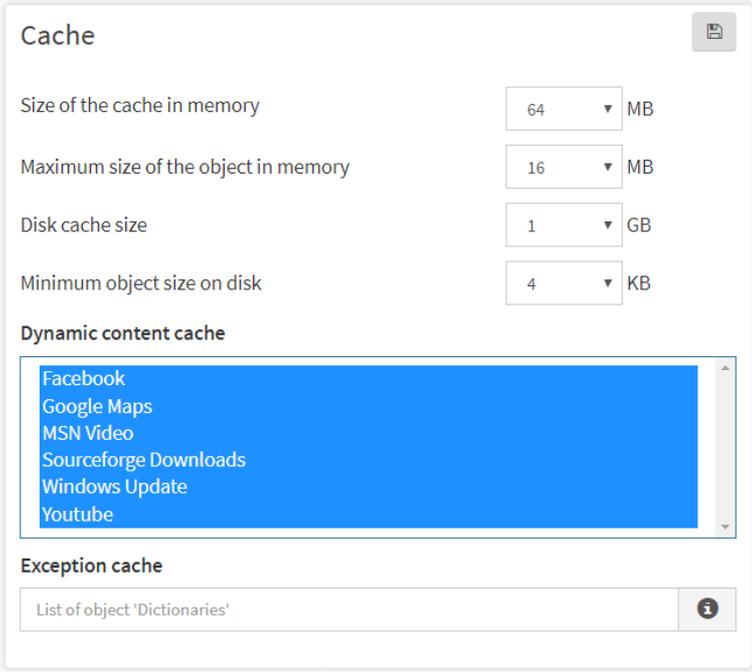
Existem conteúdos que são disponibilizados pelos servidores WEB de forma dinâmica e distribuída, são os chamados CDN (Content Delivery Network). Esse recurso utiliza uma tecnologia que responde a requisição do usuário pelos servidores web mais próximos da sua localização geográfica.

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 sistema de proxy concatena os fragmentos do conteúdo solicitado e guarda a cache mesmo de origens diversas.

[Recursos]

- Facebook
- Google Maps
- MSN Video
- Source forge Downloads
- Windows Update, YouTube.

Suporte a “Exception cache”, configurável através dos objetos “Dictionary” por uso de expressões regulares.



Cache

Size of the cache in memory: 64 MB

Maximum size of the object in memory: 16 MB

Disk cache size: 1 GB

Minimum object size on disk: 4 KB

Dynamic content cache

- Facebook
- Google Maps
- MSN Video
- Sourceforge Downloads
- Windows Update
- Youtube

Exception cache

List of object 'Dictionaries'

[Hierarquia]

No quadro [Hierarchy] temos o recurso de configuração de redirecionamento do tráfego Proxy. Um modelo de Proxy hierárquico, que atua no modelo “Proxy Parent”.

Algumas estruturas com subredes exigem que o tráfego de cada subrede 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 cache local antes do redirecionamento do acesso à internet.

Suporte à integração com sistemas DLP (Data Loss Prevention), através da hierarquia de Proxy, redirecionando o tráfego para aplicação de filtros e tratamentos dos pacotes HTTP/HTTPS por aplicações de Antivírus HTTP.

Hierarchy

Enabled

IP Address: 192.168.101.212 ⓘ Port: 33128 ⓘ

Authenticated: Enabled

Type: User Manual

User: blockbit.utm Password:



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

User Authentication Method → Este método solicita autenticação diretamente ao usuário final, através de autenticação “basic” via browser.
Manual Authentication Method → Este método solicita autenticação “mestra” diretamente ao Proxy local.

5 Web Filter

O serviço do Web Filter funciona como uma segunda camada de segurança e tratamento de dados 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 e Http/s são repassadas por um servidor Proxy, antes de solicitar os dados ao servidor de aplicações remoto, ele redireciona algumas informações da requisição (url, usuário e endereço IP do usuário) para o serviço de Web Filter.

O Blockbit UTM possui uma base de dados (Secure Web Gateway) que contempla mais de 48 milhões de endereços de URL's e URI's classificados em 88 categorias, e mais uma categoria adicional "Sites não catalogados".

Estas informações, em conjunto com a inspeção SSL, permitem controlar totalmente o acesso ao conteúdo de tráfego online dos usuários da rede, o que pode ser configurado por usuário, grupos de usuários, endereço IP, largura de banda, prioridade de conexão, links. Você também pode determinar limites para tamanho de arquivos para download, upload, execução de aplicações web, tempo de navegação e outros.

A Habilitação do serviço dispõe da configuração da "Página de Bloqueio" e a integração com o serviço "Captive Portal". E a parametrização dos perfis Web Filter que caracterizam os modelos de "Compliances" para integração as "Políticas de Segurança".

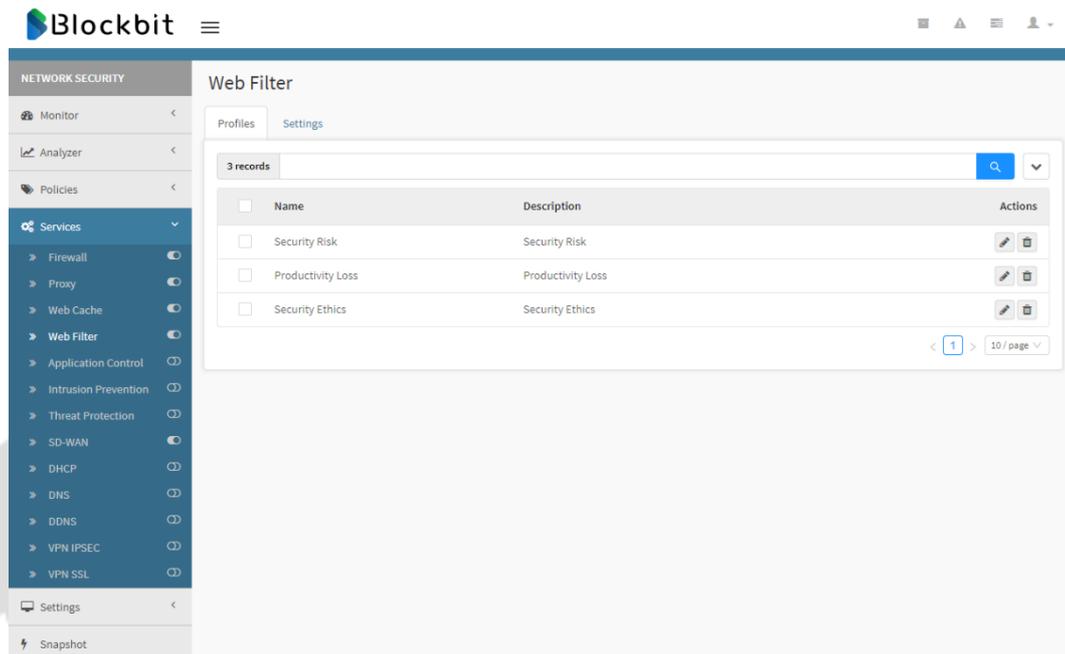
Os Recursos dos perfis Web Filter são classificados por tipo, são eles:

- Busca
 - Controle de login por domínio para os serviços Google Apps.
 - Habilitação do serviço de busca segura “ Safe Search”.
- Filtros
 - Categorias Web.
 - Filtros de Arquivos.
- Surfing Quotas
 - Cotas de tempo máximo.
 - Cotas de tráfego máximo.
 - Tamanho máximo de download.
 - Tamanho máximo de Upload.

Com base nas informações enviadas pelo Proxy Http, o Web Filter procura por filtros de busca para o “Controle de acesso ao G-Suite Google”, e habilitação “SafeSearch” para os principais buscadores da web, “Google, Yahoo e Bing”.

Integrado a uma base de Url's, pesquisa por “Categoria de Url's”, e “Tipos de conteúdo”, ainda aplica um serviço chamado “Controle de navegação”, que incluem controles de “Cotas de tempo e tráfego” e “Tamanho máximo de download e upload de arquivos”, que se aplicam através das “Políticas de segurança”. Dependendo de como as políticas estão configuradas, o Web Filter responde ao proxy se a requisição foi permitida ou bloqueada.

Para configuração do Web Filter, acesse o menu [Services] >> [Web Filter]



Recomenda-se: A habilitação do serviço [ / ] antes da sua configuração.

O recurso Web Filter foi desenvolvido usando um critério de usabilidade para facilitar sua implementação. Pensando nisso o Blockbit UTM contempla alguns “Perfis” pré-configurados.

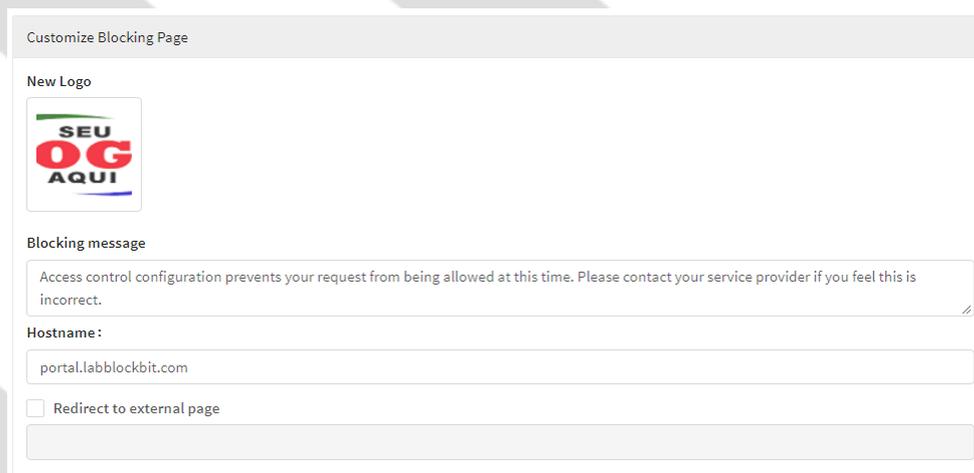
7.1 Configurações Web Filter

Nesta seção configura-se a personalização da página de bloqueio devolvida pelo Web Filter às requisições de navegação web “Não Autorizadas”.

[Personalização da página de bloqueio]

No quadro [Customize blocking page] temos um recurso que permite customizar a página de bloqueio que é devolvida aos usuários da rede referente aos acessos “Não Autorizados” do tráfego Web. (interceptados pelo proxy).

Clique em Upload [] para carregar a Imagem LOGOTIPO da sua empresa



Customize Blocking Page

New Logo

Blocking message

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Hostname:

portal.labblockbit.com

Redirect to external page

[Blocking message]

Defina a mensagem de bloqueio que será exibida para seu usuário final. Ex.: “Access control Configuration prevents your request from being Allowed at this time. Please contact your system Administration if you feel this is incorrect.”.

“A configuração do controle de acesso impede que sua solicitação seja permitida neste momento. Entre em contato com a administração do sistema se achar que isso está incorreto.”.

[Hostname]

Se refere ao nome FQDN do certificado de serviço. [System] >> [Certificates] aba [Services] habilitado no serviço de “Autenticação”. Ex.: “portal.labblockbit.com”

[✓] Redirect to external page

Habilita o redirecionamento da página de bloqueio para uma página externa personalizada.

 Para os casos das tentativas de acesso WEB não autorizado, ou seja, definidos por meio das políticas de segurança com a ação de “Bloqueio” selecionada, o sistema retorna a tela de “Bloqueio” abaixo, com a mensagem especificada no quadro acima.



Access Denied



| | |
|-----------------|--------------------------|
| URL | https://www.kproxy.com/ |
| Policy | Navegação WEB Controlada |
| Category | Proxy Avoidance |
| App | - |
| Reason | Time surfing quota |

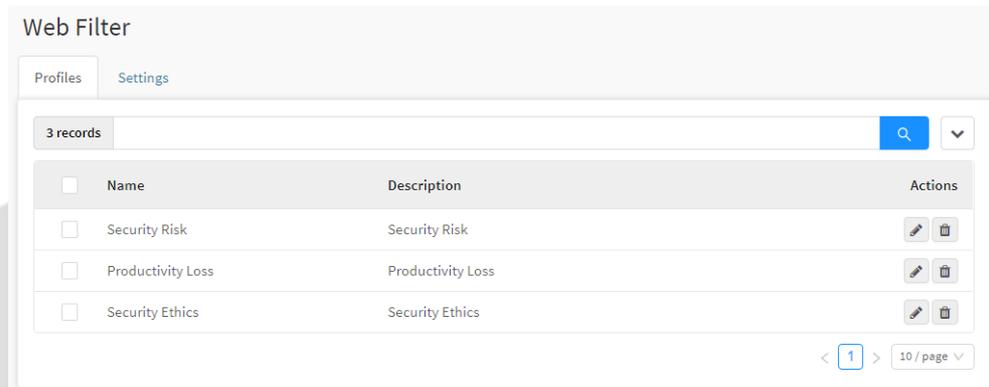
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Powered by BLOCKBIT®
portal.labblockbit.com
20/Mar/2020:15:53:40 -0300

 NÃO se esqueça de APLICAR A Fila de comandos []

7.2 Perfis Web Filter

Neste tópico vamos conhecer os perfis populados pelo sistema. Clique na aba [Profiles].



| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|-------------------|-------------------|---|
| <input type="checkbox"/> | Security Risk | Security Risk |   |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss |   |
| <input type="checkbox"/> | Security Ethics | Security Ethics |   |

Vale ressaltar que a implementação ÚNICA e EXCLUSIVA dos perfis populados integrados a compliance das “Políticas de segurança” não caracteriza que seu ambiente esteja com a melhor política “Secure Web Gateway” implementada.

Esse conjunto de perfis tem como finalidade única, auxiliar a fase inicial de implementação e não tem intenção nenhuma de se propor como uma política final de Web filter. Podemos aplicá-lo como uma modalidade de Raio-X da rede.

Esses perfis visam a implementação básica de segurança e gerenciamento no controle do acesso à internet no acesso a categorias de sites consideradas inapropriadas e inseguras ao ambiente corporativo.

[Security Risk]

Bloqueio de “Sites e Url’s” de categorias com conteúdo inapropriado e que caracterize risco de segurança.

| Categories | |
|------------------------|-------------------------------|
| Information Technology | Internet Communication |
| Hacking | Web Chat |
| Proxy Avoidance | Web Mail |
| Web hosting | Potentially Unwanted Software |
| Computer Security | Malicious Web Sites |
| Spynwares | |

[Productivity Loss]

Bloqueio de “Sites” e “Url’s” de categorias com conteúdo inapropriado e que caracterize perda de produtividade.

| Categories | |
|---------------------------------|-------------------------------------|
| Entertainment | Society and Lifestyles |
| MP3 and Audio Download Services | Alcohol na Tobacco |
| Games | Gay or Lesbian or Bisexual Interest |
| Shopping | Personals and Dating |
| Internet Auctions | Restaurants and Dining |
| Real Estate | Hobbies |
| Society and Lifestyles | Social Networking and Personal Sit |
| Sports | Sport Hunting and Gun Clubs |

[Security Ethics]

Bloqueio de “Sites” e “Urls” de categorias com conteúdo inapropriado e que caracterize problemas de segurança ética.

| Categories | |
|-----------------------|-----------------------------|
| Adult Material | Abused Drugs |
| Adult Content | Supplements and Inregulated |
| Nudity | Marijuana |
| Sex | Gambling |
| Sex Education | Illegal or Questionable |
| Lingerie and Swimsuit | Pedophilia |
| Tastless | Militancy and Extremist |
| Violence | Racism and Hate |

Vamos exemplificar a criação de alguns perfis “Web Filter” a fim de abranger os demais recursos de gerenciamento e controle no acesso aos serviços Web.

7.3 Entendendo a criação dos Perfis Web Filter

Perfil Web: Conjunto regras que incluem: Os filtros de “Categorias de sites” classificados pelo módulo do Web Filter, as “Categorias customizadas” pelo administrador, e os “Controles de navegação”.

Na seção anterior “Inspeção SSL” você aprendeu que a aplicação da interceptação SSL, se aplica por meio das “Compliances das políticas de segurança” para fins de inspeção e bloqueio integrados aos serviços de segurança e Web Proxy.



Boa prática:

Recomenda-se que a configuração dos perfis de filtros Web Filter seja definida baseada em um modelo de conformidade de políticas por grupo de usuários com as mesmas finalidades ou aplicabilidades no acesso à internet.

Ex.: “**Grupos de departamento: Financeiro, Administrativo, Controladoria, Suporte T.I, Marketing, Comercial, Sac, Recursos Humanos...**”.

Você pode definir diferentes “Perfis” um para cada “Depto” da sua empresa, tendo como base as atividades nos acessos a serviços Web relacionados com as suas atividades.



Os Perfis para “Inspeção Web Filter” se aplicam por meio das “Políticas de Segurança”.

Os Filtros de inspeção para as ações de “Bloqueio” dependem da integração com um perfil de “Inspeção SSL” para o protocolo Https.

Para saber como integrar esses recursos consulte o capítulo “Políticas de Segurança – SWG”.

7.3.1 Perfil Web Filter 1 – Navegação Inapropriada

Descrição da compliance Web Filter 1:

Adicionar um perfil de acesso “Web” para todos os grupos de usuários da rede, sem exceção.

Defina uma lista de categorias que considere “Risco de segurança e Ética” para as atividades em ambientes corporativos e defina-as com ação de “Bloqueio”. Considere permitir acesso as URL’s e Sites “[Não catalogadas](#)” e a categoria “[Mecanismo buscas e portais](#)”.

Filtre também as ações de pesquisas dos principais navegadores Web, para “Não responder” as pesquisas de vídeos e imagens com conteúdo considerados “Inapropriados”. – Recurso SafeSearch.

Lista de categorias de “Sites e Url’s” classificados com possível conteúdo inapropriado e que caracteriza risco de segurança e ética.

| Categories [Security Ethics] | |
|------------------------------|-----------------------------|
| Adult Material | Drugs |
| Adult Material | Abused Drugs |
| Adult Content | Supplements and Inregulated |
| Nudity | Marijuana |
| Sex | Illegal or Questionable |
| Gambling | Illegal or Questionable |
| Gambling | Pedophilia |
| Games | |

| Categories [Security Risk] | |
|----------------------------|-------------------------------|
| Information Tecnology | Potentially Unwanted Software |
| Hacking | Potentially Unwanted Software |
| Proxy Avoidance | Malicious Web Sites |
| | Spyware |
| | |

Para configurar um Perfil Web, preencha os campos de configuração baseado nos tipos de filtros que deseja aplicar em uma determinada política.

Clique em Create Profile [],

Abaixo as especificações de configuração do serviço para cada quadro:

[General]

General

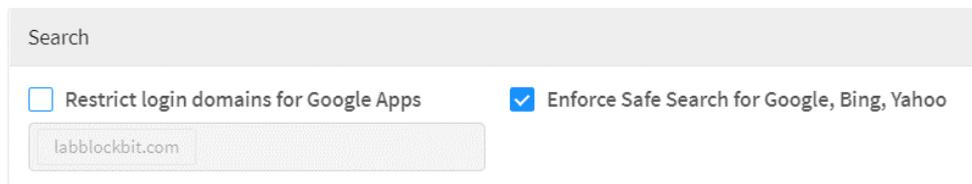
*** Name**

Description

Name: Digite um nome para o perfil Web. Ex.: “Web Inapropriada [Safety Ethics Risk]” {requisito obrigatório}.

Description: Defina uma descrição para identificação do perfil Web. Ex.: Ex.: “Web Inapropriada [Safety Ethics Risk]” {requisito obrigatório}.

[Search]



Search

Restrict login domains for Google Apps Enforce Safe Search for Google, Bing, Yahoo

labblockbit.com

[] Restricit login domains for Google Apps.

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

Caso de Uso: Sua empresa contrata a Google para hospedar seus emails com direitos de usar aplicações G- Suíte Google para seu domínio corporativo, logo, o administrador pode optar em “proibir” seus usuários de usar aplicações pessoais.

Ex.: Se o campo domínio for preenchido com o valor “seudominio.com” os usuários só poderão se autenticar nos serviços da Google com sua conta corporativa “[usuário@seudominio.com](#)”. Se algum usuário tentar acessar os serviços da Google com sua conta pessoal “[user@gmail.com](#)”, o sistema retornará a seguinte mensagem de “Bloqueio”.



Habilite este serviços de restrição de domínio para o Google Apps, se a compliance das políticas de acesso para este “Perfil – grupo”, for: “Acesso restrito aos serviços G- Suite da Google para os domínios declarados”.

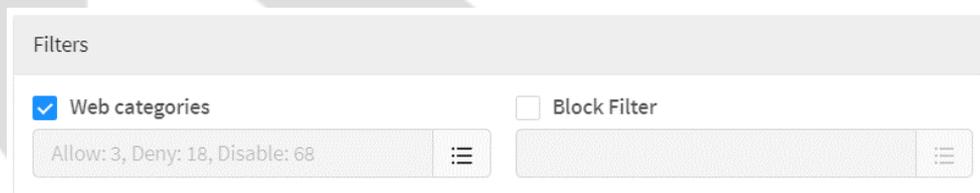
[✓] Enforce Safe Search for Google, Bing, Yahoo

Suporte aos filtros SafeSearch 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 navegadores web.

Este recurso de pesquisa segura, se aplica aos principais buscadores da Web “Google, Yahoo e Bing”.

Habilite este serviço de restrição de pesquisas a conteúdos inapropriados, se a compliance das políticas de acesso para este “Perfil – grupo”, for: “Impedir que sites com conteúdo inapropriado apareçam nos resultados de pesquisa dos usuários.

[Filters]



[✓] Web Categories

Seleção das categorias Web, que contempla o total de 88 categorias catalogadas na base SWG, uma base de reputação de Sites, Url's, diretórios e arquivos (+) 1 categoria de “Sites não catalogados”. Também contempla uma opção para “Customizar” uma base de Url's a partir do cadastro de objetos do tipo “Dicionários”.

As ações “Recusado”; “Permitidos” e/ou “Desabilitados” sobre o acesso as Url's, dependem do perfil de configuração de cada categoria web, ou seja, a habilitação do “status” da categoria para o respectivo perfil, associada a uma “Política de segurança”.

Para “Aplicar” o filtro desejado, inicie desabilitando todas as categorias. Depois selecione as categorias permitidas para aplicação do filtro “Safe Search”. Em seguida selecione as categorias do grau de risco para o perfil da compliance definida, e altere seu “Status” para ação de bloqueio → “[Recusado/ Deny]”.

Agora Clique em [Save] para atualizar o Status das categorias neste perfil.

Add Category ✕

All

| | |
|-----------------------------|-----------|
| Uncategorized Sites | Allow ▼ |
| ▼ Abortion | Disable ▼ |
| Pro-life | Disable ▼ |
| Pro-Choice | Disable ▼ |
| Activism Groups | Disable ▼ |
| ▼ Adult Material | Deny ▼ |
| Adult Content | Deny ▼ |
| Nudity | Deny ▼ |
| Sex | Deny ▼ |
| Sex Education | Deny ▼ |
| Lingerie and Swimsuit | Deny ▼ |
| ▼ Business and Economy | Disable ▼ |
| Financial Data and Services | Disable ▼ |
| ▼ Drugs | Deny ▼ |
| Abused Drugs | Deny ▼ |
| Prescribed Medications | Allow ▼ |

[] File Filter

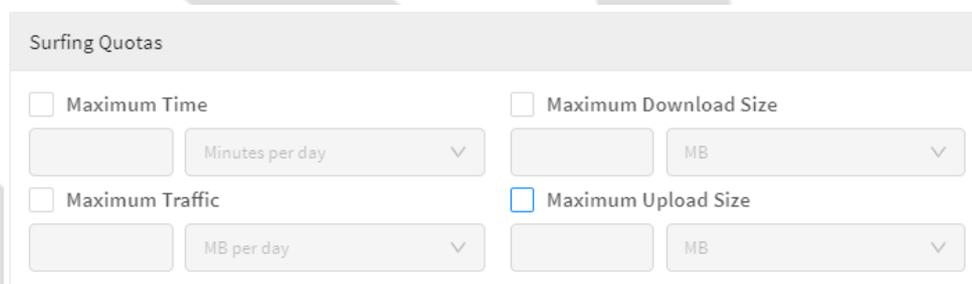
Seleção de objetos por “Content-type” ou por “extensão” do arquivo, com a finalidade de filtrar os tipos de conteúdo de arquivos potencialmente sujeitos a “Infecções” por “Malware”. Ex.: “zip; arj; tar; tgz; rar”; “exe; vb; vbs; bat”.

Identificando arquivos contidos nas listas habilitadas no filtro, associadas a uma política de segurança seja por “Content-type” ou por “extensão” do arquivo, seu acesso é bloqueado.



[Surfing Quotas]

Recurso de controle de navegação web, este recurso pode ser aplicado como uma espécie de tarifação. Este modelo de controle contempla um conjunto de critérios de tarifação: “Cota de tempo e tráfego e tamanho máximo de download e upload”.



[] Maximum Time

Limite máximo de “Tempo” de navegação [min/ dia] ou [hora/ dia] para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “1[uma] hora por dia”.

[] Maximun Traffic

Limite máximo do “Tráfego” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “500 MB por dia”.

[] Maximum Download

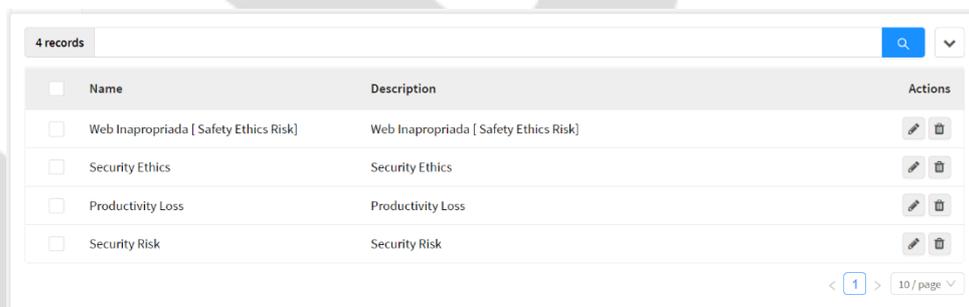
Tempo máximo de “Download” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex. “300 MB”.

[] Maximun Upload

Limite máximo de “Upload” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “100 MB”.

Habilite e configure este recurso, se a compliance das políticas de acesso para este “Perfil – grupo”, for: Aplicar controle de navegação tarifada por “Cota de tempo”, “Cota de tráfego” e/ ou “Tamanho limites de Download e Upload”.

Depois clique em [Save].



| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|--|--|---------|
| <input type="checkbox"/> | Web Inapropriada [Safety Ethics Risk] | Web Inapropriada [Safety Ethics Risk] | |
| <input type="checkbox"/> | Security Ethics | Security Ethics | |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss | |
| <input type="checkbox"/> | Security Risk | Security Risk | |

< 1 > 10 / page

7.3.2 Perfil Web Filter 2 – Navegação Segura

Descrição da compliance:

Adicionar um perfil “Web” para todos os usuários da Rede. Ex.: Grupo all@seudominio.com”.

Considere permitir o acesso irrestrito a qualquer Site ou URL , inclusive os sites “Não Catalogados”.

Para tornar a navegação dos usuários segura, considerar os filtros de “Arquivos” para o bloqueio de “Downloads ou execução” para todos os “tipos de conteúdo/ extensões” de arquivos sujeitos a infecções por vírus e malware. .Ex.: “.exe; .bat; .vb; .vbs; .zip, outros”

Para configurar um Perfil Web, preencha os campos de configuração baseado na “Descrição da compliance” e nos “tipos de filtros” especificados para aplicação da política definida.

Clique em Create Profile [,

Abaixo as especificações de configuração do serviço para cada quadro:

[General]

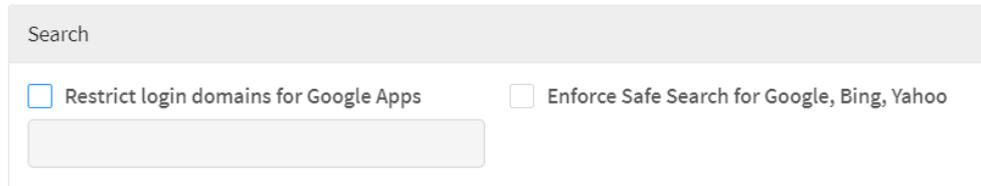


| General | |
|--------------------|---|
| * Name | <input type="text" value="Navegação Segura [Safe Browsing]"/> |
| Description | <input type="text" value="Navegação Segura [Safe Browsing]"/> |

Name: Digite um nome para o perfil Web. Ex.: “Navegação Segura [Safe Browsing]” {requisito obrigatório}.

Description: Defina uma descrição para identificação do perfil Web. Ex.: “Navegação Segura [Safe Browsing]”.

[Search]



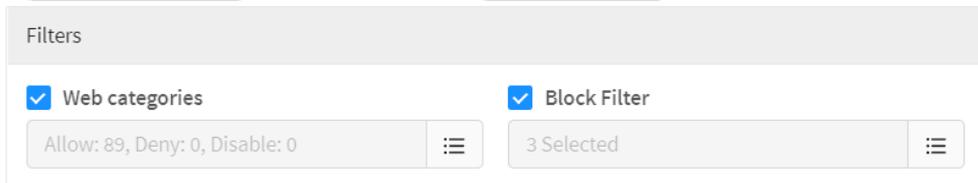
[] Restricit login domains for Google Apps.

Para este perfil: “Não Habilitar”.

[] Enforce Safe Search for Google, Bing, Yahoo

Para este perfil: “Não Habilitar”.

[Filters]



[] Web Categories

Habilite o recurso de filtro “[Web Categories]”

As ações “Recusado”; “Permitidos” e/ou “Desabilitados” sobre o acesso as Url’s, dependem do perfil de configuração de cada categoria web, ou seja, a habilitação do “status” da categoria para o respectivo perfil, associada a uma “Política de segurança”.

Selecione Todas as 89 categorias Web, com perfil de ação do tipo: “Permitir / Allow”.

Add Category X

All ▼ 🔍 ▼

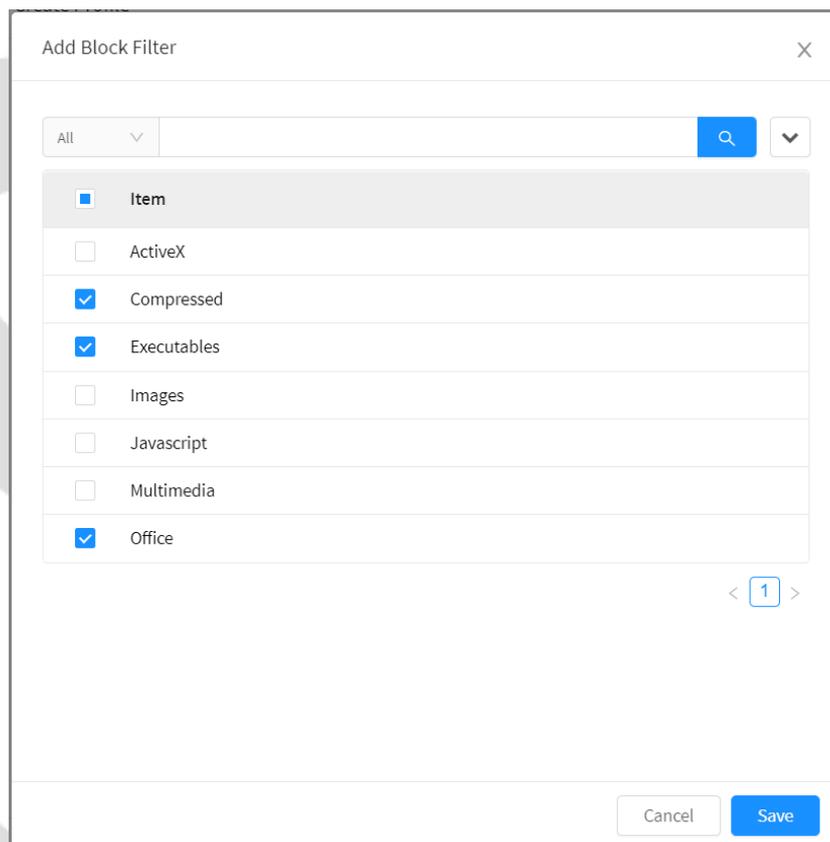
| | |
|---------------------------|---------|
| Uncategorized Sites | Allow ▼ |
| ▶ Abortion | Allow ▼ |
| ▶ Activism Groups | Allow ▼ |
| ▶ Adult Material | Allow ▼ |
| ▶ Business and Economy | Allow ▼ |
| ▶ Drugs | Allow ▼ |
| ▶ Education | Allow ▼ |
| ▶ Entertainment | Allow ▼ |
| ▶ Gambling | Allow ▼ |
| ▶ Games | Allow ▼ |
| ▶ Government | Allow ▼ |
| ▶ Health | Allow ▼ |
| ▶ Illegal or Questionable | Allow ▼ |
| ▶ Information Technology | Allow ▼ |
| ▶ Internet Communication | Allow ▼ |
| ▶ Job Search | Allow ▼ |

Custom Cancel Save

[√] File Filter

Habilite o recurso de filtro “[File Filter]”

Selecione os agrupamentos dos tipos de grau de risco para o perfil da compliance definida como conteúdos de arquivos potencialmente sujeitos a “Infecções” por “vírus e Malware”. Ex.: “zip; arj; tar; tgz; rar”; “exe; vb; vbs; bat”.



[Surfing Quotas]

Surfing Quotas

Maximum Time Maximum Download Size

Minutes per day MB

Maximum Traffic Maximum Upload Size

MB per day MB

Para este perfil: “Não Habilitar”.

Depois clique em [Save].

5 records

| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|--|--|---------|
| <input type="checkbox"/> | Navegação Segura [Safe Browsing] | Navegação Segura [Safe Browsing] | |
| <input type="checkbox"/> | Web Inapropriada [Safety Ethics Risk] | Web Inapropriada [Safety Ethics Risk] | |
| <input type="checkbox"/> | Security Ethics | Security Ethics | |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss | |
| <input type="checkbox"/> | Security Risk | Security Risk | |

< 1 > 10 / page

7.3.3 Perfil Web Filter 3 – Controle G Suite Google

Descrição da compliance:

Adicionar um perfil “Web” para todos os usuários da rede, aplicando filtros de restrição de “domínios” no login ao “G-Suite da Google”.

Aplicar filtro de acesso sob a categoria de “Mecanismo buscas e Portais” e lista de URL’s customizadas para o domínio “google.com”, com a finalidade de não permitir acesso aplicativos e ferramentas google com o uso de conta pessoal.

Considere permitir o acesso irrestrito a lista de Sites ou URL’s. “Não Catalogados”.

Lista de categorias de “Sites e URL’s” classificados de acordo a compliance definida.

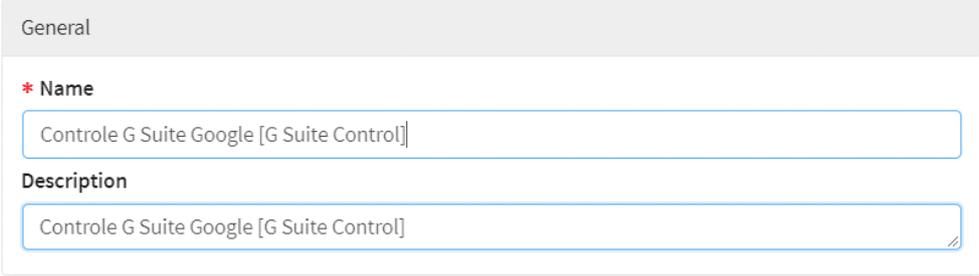
| Categories (G-Suite Google) | |
|--|----------------------------|
| Custom | Information Technology |
| Urls G-Suite da Google. (Obj. Dictionary *.google.com*) | Search Engines and Portals |
| Uncategorized Sites | |
| Uncategorized Sites | |
| | |

Para configurar um Perfil Web, preencha os campos de configuração baseado na “Descrição da compliance” e nos “Tipos de filtros” especificados para aplicação da política definida.

Clique em Create Profile [],

Abaixo as especificações de configuração do serviço para cada quadro:

[General]



General

* Name

Controle G Suite Google [G Suite Control]

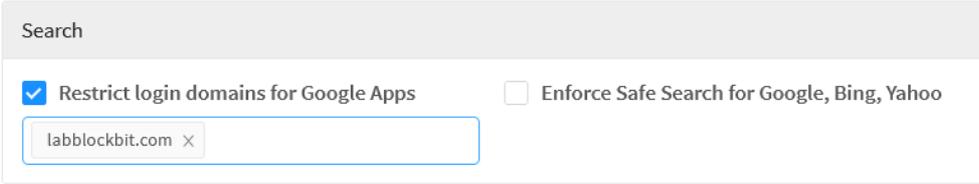
Description

Controle G Suite Google [G Suite Control]

Name: Digite um nome para o perfil Web. Ex.: “Controle G Suite Google [G Suite Control]” {requisito obrigatório}.

Description: Defina uma descrição para identificação do perfil Web. Ex.: “Controle G Suite Google [G Suite Control]” {requisito obrigatório}.

[Search]



Search

Restrict login domains for Google Apps Enforce Safe Search for Google, Bing, Yahoo

labblockbit.com x

[] Restricit login domains for Google Apps.

Especificar o nome do domínio com permissão de acesso aos Apps G Suite Google. Ex.: “labblockbit.com”.

[] Enforce Safe Search for Google, Bing, Yahoo

Para este perfil: “Não Habilitar”.

[Filters]



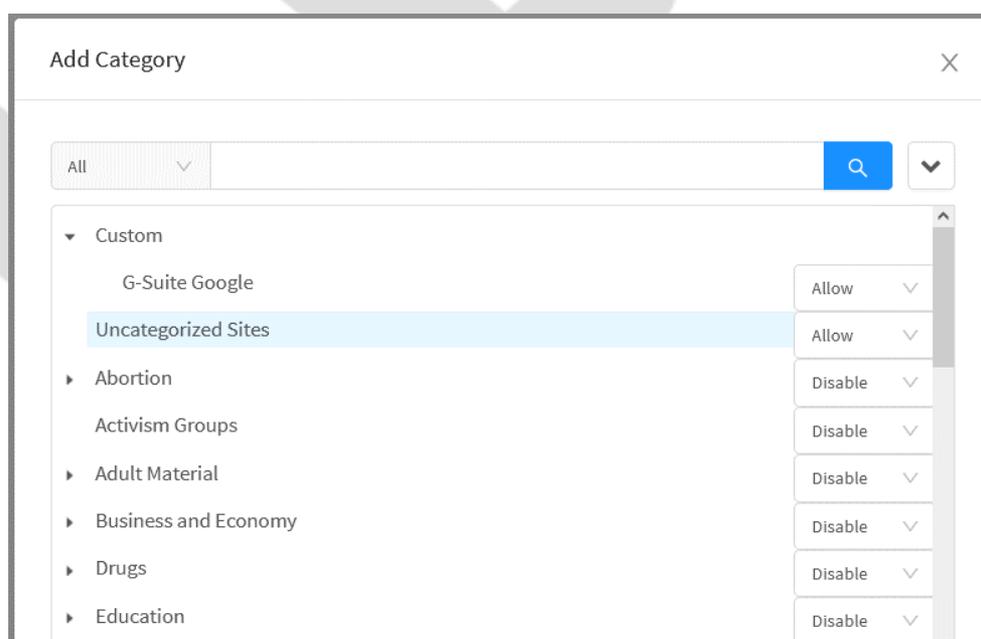
[√] Web Categories

Habilite o recurso de filtro “[Web Categories]”.

As ações “Recusado”; “Permitidos” e/ou “Desabilitados” sobre o acesso as Url’s, dependem do perfil de configuração de cada categoria web, ou seja, a habilitação do “status” da categoria para o respectivo perfil, associada a uma “Política de segurança”.

Filtre o status “Allow” e altere seu status para “Disable”. Depois selecione as categorias para o perfil da compliance definida e altere seu “Status” para ação de permissão → “[Permitir/ Allow]”.

Clique em [Save] para atualizar o Status das categorias neste perfil.



[Surfing Quotas]

Surfing Quotas

| | |
|--|--|
| <input type="checkbox"/> Maximum Time | <input type="checkbox"/> Maximum Download Size |
| <input type="text"/> Minutes per day | <input type="text"/> MB |
| <input type="checkbox"/> Maximum Traffic | <input type="checkbox"/> Maximum Upload Size |
| <input type="text"/> MB per day | <input type="text"/> MB |

Para este perfil: “Não Habilitar”.

Depois clique em [Save].

6 records

| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|---|---|---------|
| <input type="checkbox"/> | Controle G Suite Google [G Suite Control] | Controle G Suite Google [G Suite Control] | |
| <input type="checkbox"/> | Navegação Segura [Safe Browsing] | Navegação Segura [Safe Browsing] | |
| <input type="checkbox"/> | Web Inapropriada [Safety Ethics Risk] | Web Inapropriada [Safety Ethics Risk] | |
| <input type="checkbox"/> | Security Ethics | Security Ethics | |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss | |
| <input type="checkbox"/> | Security Risk | Security Risk | |

< 1 > 10 / page

7.3.4 Perfil Web Filter 4 – Navegação Wi-Fi Corp – [Surf Control]

Descrição da compliance:

Adicionar um perfil “Web” para todos os usuários da Rede Wi-Fi Corp Free. Ex.: Grupo “all@labblockbit.com”.

Considere permitir o acesso irrestrito a qualquer Site ou URL , inclusive os sites “Não Catalogados” . Exceto as categorias de sites de Risco de segurança ética e conteúdos maliciosos que possam comprometer a gerência da rede corporativa.

Lista de categorias de “Sites e URL’s” classificados com possível conteúdo inapropriado e que caracteriza risco de segurança e ética.

| | |
|------------------------------|-------------------------------|
| Categories [Security Ethics] | |
| Adult Material | Drugs |
| Adult Material | Abused Drugs |
| Adult Content | Supplements and Inregulated |
| Nudity | Marijuana |
| Categories [Security Risk] | |
| Illegal Questionable | Potentially Unwanted Software |
| Illegal Questionable | Potentially Unwanted Software |
| Pedophilia | Malicious Web Sites |
| Information Technology | Spyware |
| Proxy Avoidance | |

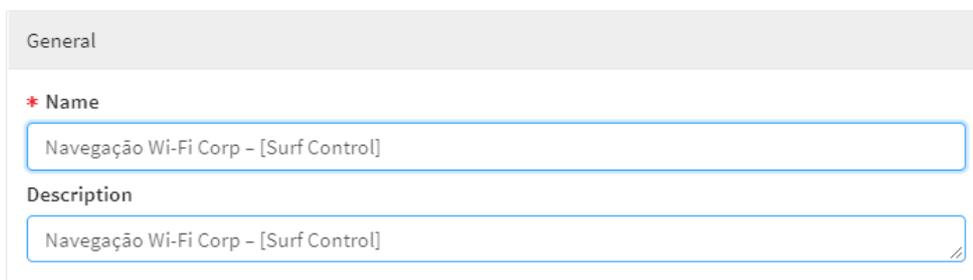
Este perfil deve atender a “Rede Wi-Fi Corp”, no entanto seu acesso deve ser limitado a 2 horas de conexão ou 500 Mb de tráfego por dia.

Para configurar um Perfil Web, preencha os campos de configuração baseado na “Descrição da compliance” e nos “Tipos de filtros” especificados para aplicação da política definida.

Clique em Create Profile [,

Abaixo as especificações de configuração do serviço para cada quadro:

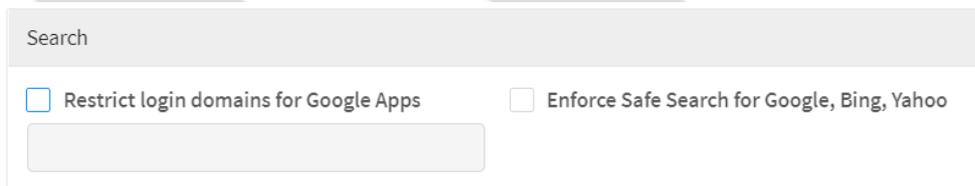
[General]



Name: Digite um nome para o perfil Web. Ex.: “Navegação Wi-Fi Corp [Surf Control]” {requisito obrigatório}.

Description: Defina uma descrição para identificação do perfil Web. Ex.: “Navegação Wi-Fi Corp [Surf Control]”.

[Search]



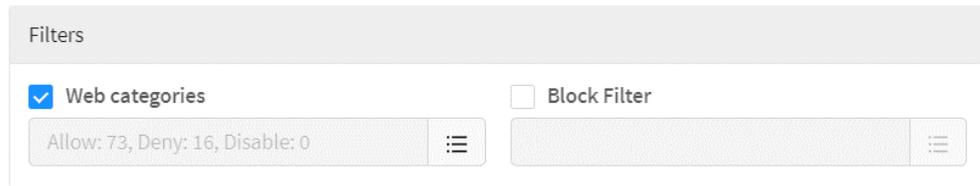
Restrict login domains for Google Apps.

Para este perfil: “Não Habilitar”.

Enforce Safe Search for Google, Bing, Yahoo

Para este perfil: “Não Habilitar”.

[Filters]



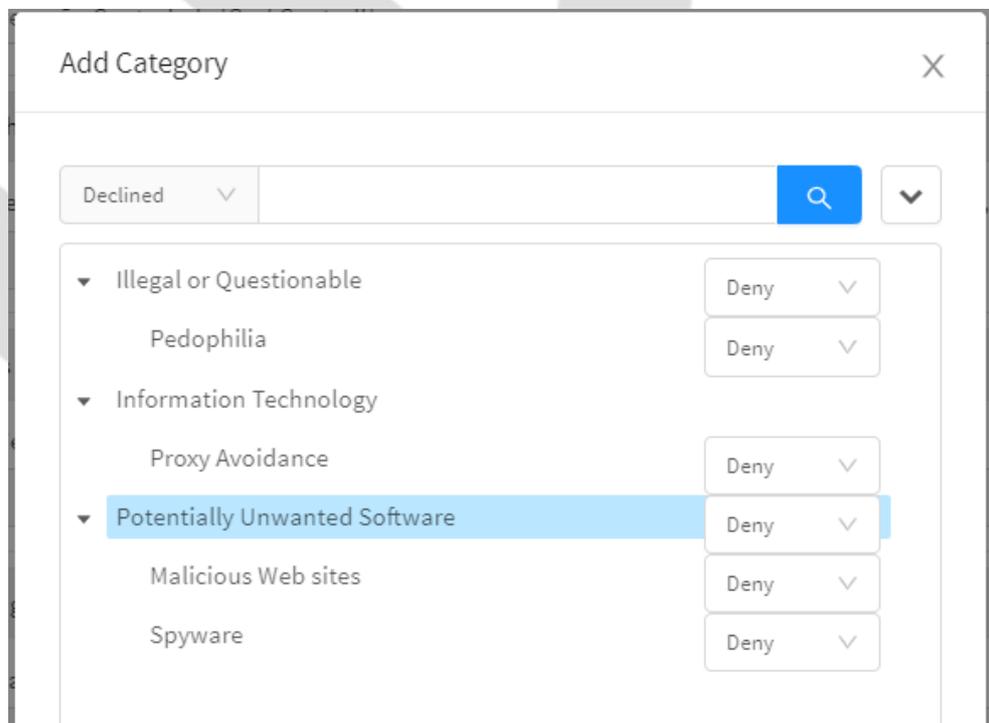
[✓] Web Categories

Habilite o recurso de filtro “[Web Categories]”.

As ações de “Bloqueio” e “Permissão” sobre o acesso as Url’s, dependem do perfil de configuração de cada categoria web, ou seja, a habilitação do “status” da categoria para o respectivo perfil, associada a uma “Política de segurança”.

Selecione as categorias do grau de risco para o perfil da compliance definida e altere seu “Status” para ação de bloqueio → “[Deny]”.

Clique em [Save] para atualizar o Status das categorias neste perfil.

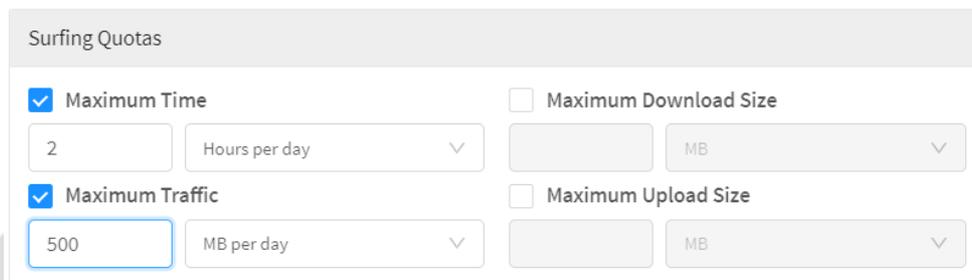


[] File Filter

Para este perfil: “Não Habilitar”.

[Surfing Quotas]

Recurso de controle de navegação web, aplicado como um espécie de tarifação.



| Surfing Quotas | | | |
|---|--|--|--|
| <input checked="" type="checkbox"/> Maximum Time | <input type="checkbox"/> Maximum Download Size | | |
| 2 Hours per day | MB | | |
| <input checked="" type="checkbox"/> Maximum Traffic | <input type="checkbox"/> Maximum Upload Size | | |
| 500 MB per day | MB | | |

[✓] Maximum Time

Limite máximo de “Tempo” de navegação [min/ dia] ou [hora/ dia] para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “2[duas] horas por dia”.

[✓] Maximun Traffic

Limite máximo do “Tráfego” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “500 MB por dia”.

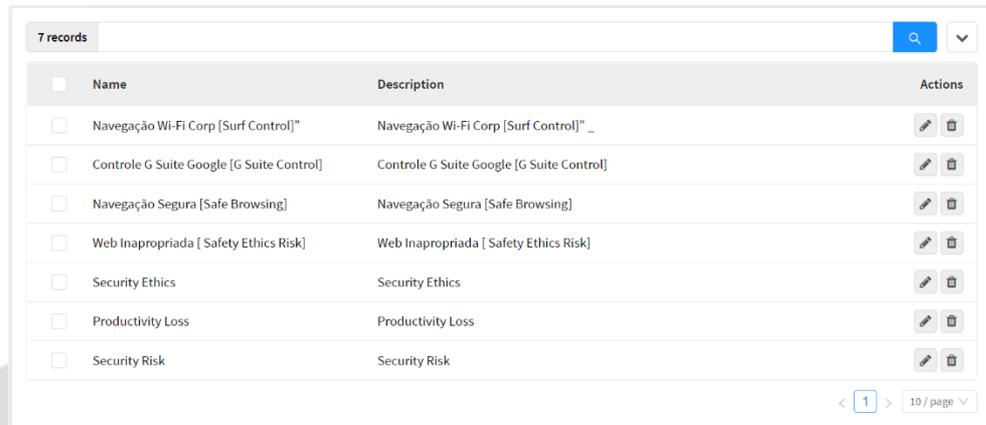
[] Maximum Download

Tempo máximo de “Download” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex. “500 MB”.

[] Maximun Upload

Limite máximo de “Upload” em [MB/ dia] de navegação para o conjunto de categorias habilitadas com Status = “Allow”. Ex.: “100 MB”.

Depois clique em [Save].



| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|---|---|---------|
| <input type="checkbox"/> | Navegação Wi-Fi Corp [Surf Control]* | Navegação Wi-Fi Corp [Surf Control]* _ | |
| <input type="checkbox"/> | Controle G Suite Google [G Suite Control] | Controle G Suite Google [G Suite Control] | |
| <input type="checkbox"/> | Navegação Segura [Safe Browsing] | Navegação Segura [Safe Browsing] | |
| <input type="checkbox"/> | Web Inapropriada [Safety Ethics Risk] | Web Inapropriada [Safety Ethics Risk] | |
| <input type="checkbox"/> | Security Ethics | Security Ethics | |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss | |
| <input type="checkbox"/> | Security Risk | Security Risk | |

7 records

< 1 > 10 / page

7.3.5 Perfil Web Filter 5 – Navegação Rede Wi-Fi [Safe Browsing]

Descrição da compliance:

Adicionar um perfil “Web” para todos os usuários da Rede Wi-Fi Guest. Ex.: “Grupo → guest@guest.com”

Considere permitir o acesso irrestrito a qualquer Site ou URL , inclusive os sites “Não Catalogados” . Exceto as categorias de sites de Risco de segurança ética e conteúdos maliciosos que possam comprometer os dispositivos ou a gerência da rede Wi-Fi Guest.

Lista de categorias de “Sites e URL’s” classificados com possível conteúdo inapropriado e que caracteriza risco de segurança e ética.

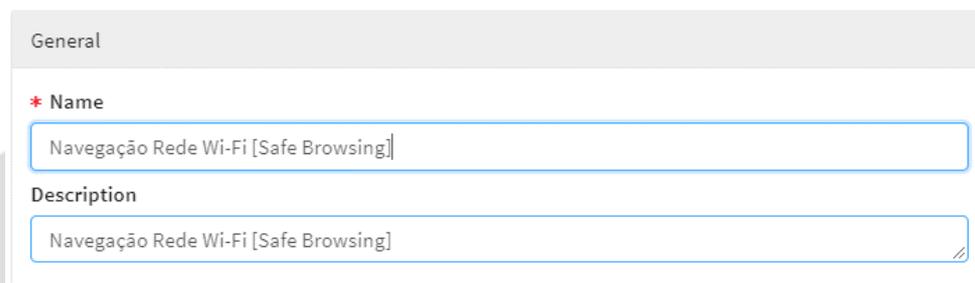
| Categories [Security Risk] | |
|----------------------------|-------------------------------|
| Illegal Questionable | Potentially Unwanted Software |
| Illegal Questionable | Potentially Unwanted Software |
| Pedophilia | Malicious Web Sites |
| Information Technology | Spyware |
| Proxy Avoidance | |

Para configurar um Perfil Web, preencha os campos de configuração baseado na “Descrição da compliance” e nos “Tipos de filtros” especificados para aplicação da política definida.

Clique em Create Profile [],

Abaixo as especificações de configuração do serviço para cada quadro:

[General]



General

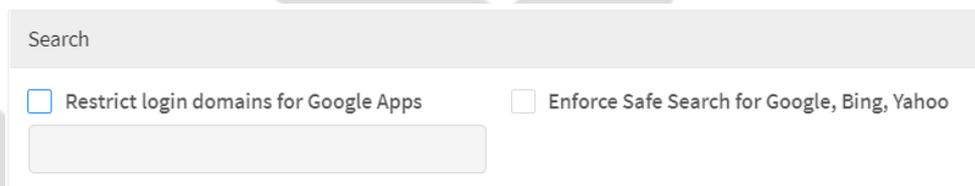
* Name
Navegação Rede Wi-Fi [Safe Browsing]

Description
Navegação Rede Wi-Fi [Safe Browsing]

Name: Digite um nome para o perfil Web. Ex.: “Navegação Rede Wi-Fi [Surf Control]” {requisito obrigatório}.

Description: Defina uma descrição para identificação do perfil Web. Ex.: “Navegação Rede Wi-Fi [Surf Control]”.

[Search]



Search

Restrict login domains for Google Apps Enforce Safe Search for Google, Bing, Yahoo

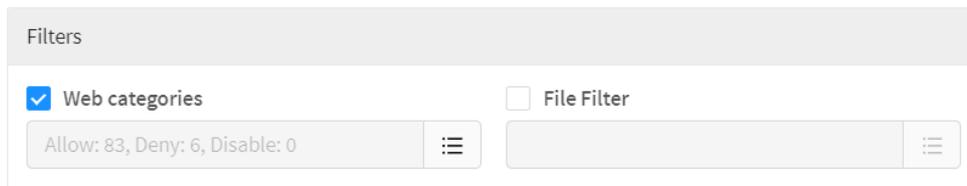
[] Restricit login domains for Google Apps.

Para este perfil: “Não Habilitar”.

[] Enforce Safe Search for Google, Bing, Yahoo

Para este perfil: “Não Habilitar”.

[Filters]



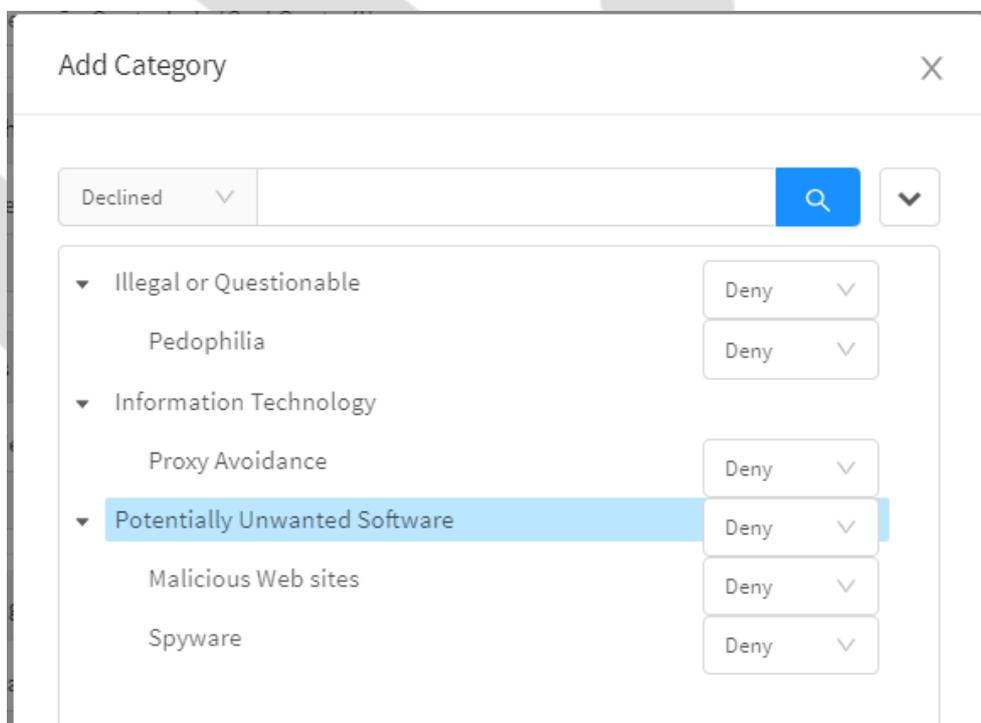
[✓] Web Categories

Habilite o recurso de filtro “[Web Categories]” .

As ações de “Bloqueio” e “Permissão” sobre o acesso as Url’s, dependem do perfil de configuração de cada categoria web, ou seja, a habilitação do “status” da categoria para o respectivo perfil, associada a uma “Política de segurança” .

Selecione as categorias do grau de risco para o perfil da compliance definida e altere seu “Status” para ação de bloqueio → “[Deny]”.

Clique em [Save] para atualizar o Status das categorias neste perfil.



[] File Filter

Para este perfil: “Não Habilitar”.

[Surfing Quotas]

Recurso de controle de navegação web, aplicado como um espécie de tarifação.

Surfing Quotas

| | |
|--|--|
| <input type="checkbox"/> Maximum Time | <input type="checkbox"/> Maximum Download Size |
| <input type="text"/> Hours per day | <input type="text"/> MB |
| <input type="checkbox"/> Maximum Traffic | <input type="checkbox"/> Maximum Upload Size |
| <input type="text"/> MB per day | <input type="text"/> MB |

[] Maximum Time

Para este perfil: “Não Habilitar”.

[] Maximum Traffic

Para este perfil: “Não Habilitar”.

[] Maximum Download

Para este perfil: “Não Habilitar”.

[] Maximum Upload

Para este perfil: “Não Habilitar”.

Depois clique em [Save].

8 records

| <input type="checkbox"/> | Name | Description | Actions |
|--------------------------|---|---|---------|
| <input type="checkbox"/> | Navegação Rede Wi-fi [Safe Browsing] | Navegação Rede Wi-fi [Safe Browsing] | |
| <input type="checkbox"/> | Navegação Wi-Fi Corp [Surf Control]" | Navegação Wi-Fi Corp [Surf Control]" _ | |
| <input type="checkbox"/> | Controle G Suite Google [G Suite Control] | Controle G Suite Google [G Suite Control] | |
| <input type="checkbox"/> | Navegação Segura [Safe Browsing] | Navegação Segura [Safe Browsing] | |
| <input type="checkbox"/> | Web Inapropriada [Safety Ethics Risk] | Web Inapropriada [Safety Ethics Risk] | |
| <input type="checkbox"/> | Security Ethics | Security Ethics | |
| <input type="checkbox"/> | Productivity Loss | Productivity Loss | |
| <input type="checkbox"/> | Security Risk | Security Risk | |

< 1 > 10 / page

