Blockbit

BLOCKBIT UTM

Políticas de Segurança

Versão 2.2

Release 2

Sobre o material

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, 1771 – Térreo
São Paulo – SP – 04717-004
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 6

1.1. Estrutura do Treinamento 6

2 POLÍTICAS DE SEGURANÇA 7

2.1 Fluxo de dados e tratamento de pacotes 8

2.2 Fundamento das políticas de segurança 9

2.3 Recursos das políticas de segurança 11

2.4 Compliances das políticas de segurança 14

2.4.1 Políticas populadas (compliance default) 15

2.5 Políticas de segurança I 17

2.5.1 Definindo grupos de políticas 17

2.5.2 Políticas de Encaminhamento (Forward) 21

2.5.3 Políticas de Mascaramento (NAT) 23

2.6 Políticas de Segurança II 30

2.6.1 Definindo grupos de políticas Web Proxy 31

2.6.2 Políticas de segurança – Web Proxy 33

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 Políticas de Segurança

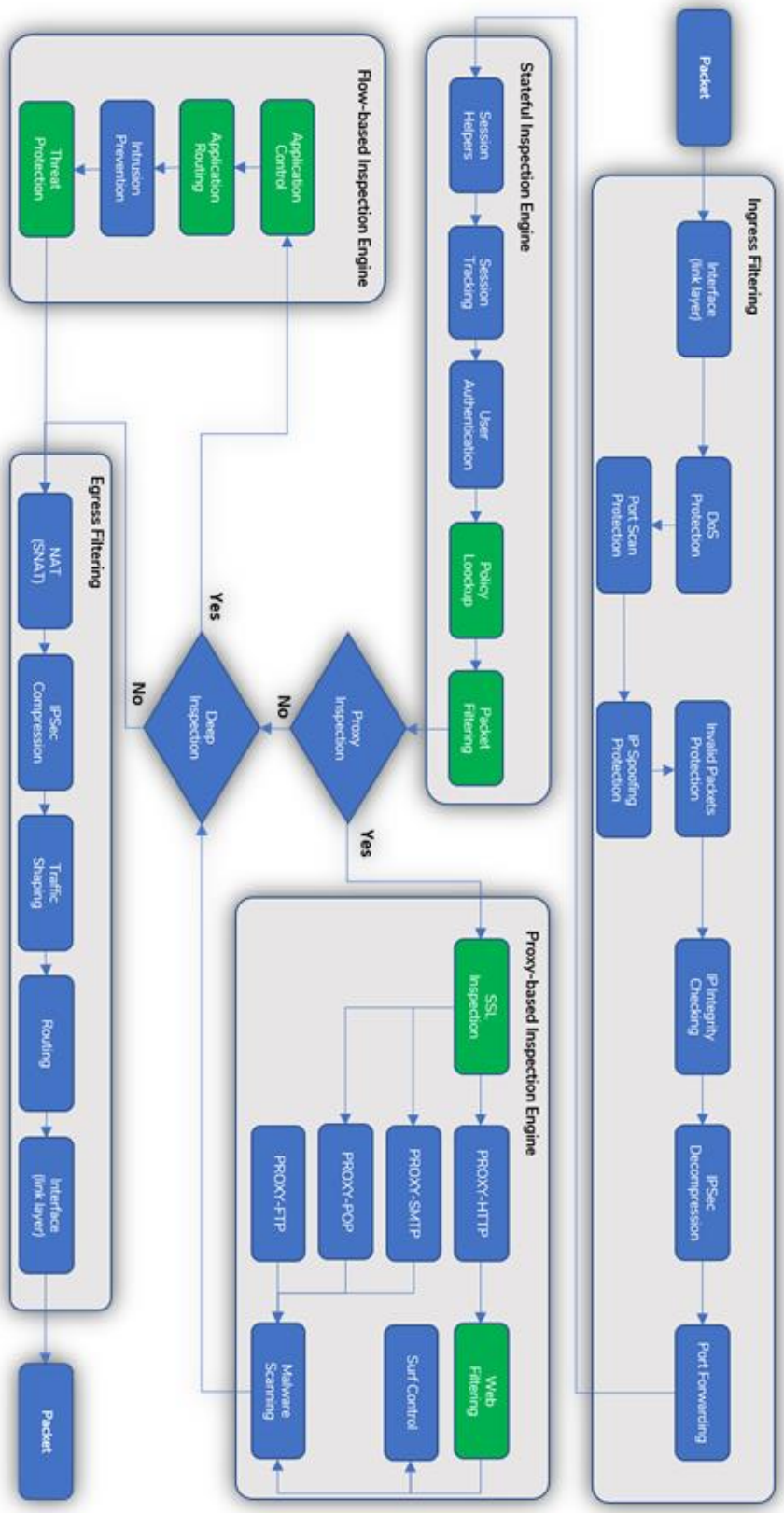
Todos os recursos de gerenciamento dos serviços de segurança Blockbit UTM, *passam por tratamento de compliances por meio das Políticas de Segurança, são eles: "Filtro de conteúdo Web, Filtros de Arquivos, Controles de navegação do tipo Cota, Tráfego e Tamanhos máximo de Download e Upload, Inspeção SSL, Inspeção IPS, ATP e APP, Garantia e prioridade de tráfego baseado em QoS (Traffic Shaping), Roteamento e Gerenciamento de links baseado em SD-Wan, Nat e Forward".*

A definição das políticas de segurança integra 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 políticas por finalidade o que facilita às pesquisas das políticas. As tags são adicionadas automaticamente pelo sistema ou o administrador pode definir uma.

As definições são idênticas para políticas no padrão IPv4 e/ ou IPv6, sofrendo alterações somente em seus endereçamentos e algumas características nativas de cada versão do protocolo.

2.1 Fluxo de dados e tratamento de pacotes



2.2 Fundamento das políticas de segurança

1) A integração dos RECURSOS em uma ÚNICA POLÍTICA.

- *NAT (Default Gateway; Source NAT)*
- *Filtros de conteúdo WEB (Proxy Http)*
- *Categorias SWG e Categorias Customizadas*
- *Controle de Tempo e Tráfego (Cota)*
- *Inspeção SSL (Protocolos Http/s, SMTP/s, FTP, POP3/s)*
- *AntiMalware*
- *Inspeção (IPS, ATP e APP Control)*
- *QoS (Traffic Shaping)*
- *Roteamento (Default Gateway/ SD-Wan)*
- *Serviços (Web Proxy ou Qualquer)*

2) A configuração ou habilitação dos serviços e recursos, "NÃO IMPLICAM" na criação de uma política de segurança.

À Exceção dos serviços "SD-Wan" 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.

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 de segurança utilizam o método de análise “FIRST MATCH WINS”.

   Na forma literal quer dizer “O 1° entre os concorrentes VENCE”.

5) As políticas de segurança são cadastradas por “Agrupamento”, “Prioridade” e suportam “Reordenação”.

   - *Políticas (IPv4 e IPv6)*
   - *Políticas Local*
   - *Políticas GSM - Global Security Management*

   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 dispositivo.

6) As ações das políticas de segurança são:

   - Allow [Permitir]
   - Deny [Bloquear]
   - Reject [Rejeitar]

Estes são os conceitos básicos que o administrador deve conhecer.

2.3 Recursos das políticas de segurança

Suporta a funcionalidade "*Multithread*" que disponibiliza o máximo proveito dos processadores. No entanto, os métodos de operação "*First Match Wins*" e a "*Ordenação por agrupamento e prioridade de políticas*" implicam diretamente no desempenho do firewall.

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 segurança atende as seguintes especificações e conjunto de filtros e condições para as tomadas de ação.

Ações	
	Allow (Permitir)
	Deny (Bloquear)
	Reject (Rejeitar)

V E R S U S...

Condições	Condições das políticas
Properties	General
	Name
	Description
	Action
	Tag's
	Policy Group
	Traffic Logging
	Schedule
	Time
	Schedule *{Period/ Date}*
Connection	Source
	Network Zone *{Agrupamento de devices}*
	Network Interface

	Country *{Geo Location – País}*
	IP Address
	MAC Address
	Destination
	IP Address
	Service
	Country *{Geo Location – País}*
	Identification
	Authenticated [Users]
	Authentication [Groups]

Inspection (*)	Inspection
	SSL Inspection (*) *{Perfil de inspeção SSL}*
	Instrusion Prevention *{Perfil de inspeção IPS – modo Server - Attacks}* *{Perfil de inspeção IPS – modo Client - Threats}*
	Threat Protection *{Perfil Anti APT e Malware Scanning}*
	Application Control *{Perfil de inspeção APP Control* *{Lista de aplicativos web 2 e de rede}*
	Web Filter *{Perfil web proxy (Http/s, FTP, SMTP/s, POP3/s)}* *{Filtro de categorias web SWG, Custom}* *{Filtro de controle de navegação}*
(*)	A Inspeção SSL é item obrigatório no tratamento das conexões do protocolo HTTPs, SMTPs e POP3s

Routing	Gateway
	NAT. *{Default Gateway/ SNAT-Endereço IP}.*
	SD-WAN *{Perfis SD-Wan: FailOver: Balanceamento: Spillover: Performance}.*
	QoS
	Traffic Shaping. *{Fila de prioridade}.* *{Parâmetros de DownStream e UPStream}*
	Flag Packets (TOS – Type of Service) *{Class ToS -Type of Service}.*

	TCP MSS. *{Maximum Segment Size}.*
	Flag Packets. (DSCP – Diff Service Code Point) *{Class DSCP – Prioridade de roteamento}* Application Routing Applications *{Perfil de inspeção APP Control}* *{Lista de aplicativos web 2 e de rede}* *SD-Wan Profile* *{Perfis SD-Wan: FailOver; Balanceamento; Spillover; Performance}.*
Flag's Packets →	*Prioridades e Roteamento dos pacotes por classes ToS e DSCP*

(*) Estes controles e filtros redirecionam o tráfego dos serviços e protocolos com intercepção via Proxies.

2.4 Compliances das políticas de segurança

O recurso das políticas de segurança foi desenvolvido usando um critério de usabilidade para facilitar sua implementação.

Já vimos os conceitos básicos que envolvem o cadastro de uma política de segurança.

Em termos de desenvolvimento de uma compliance devemos levar em consideração os critérios absolutos:

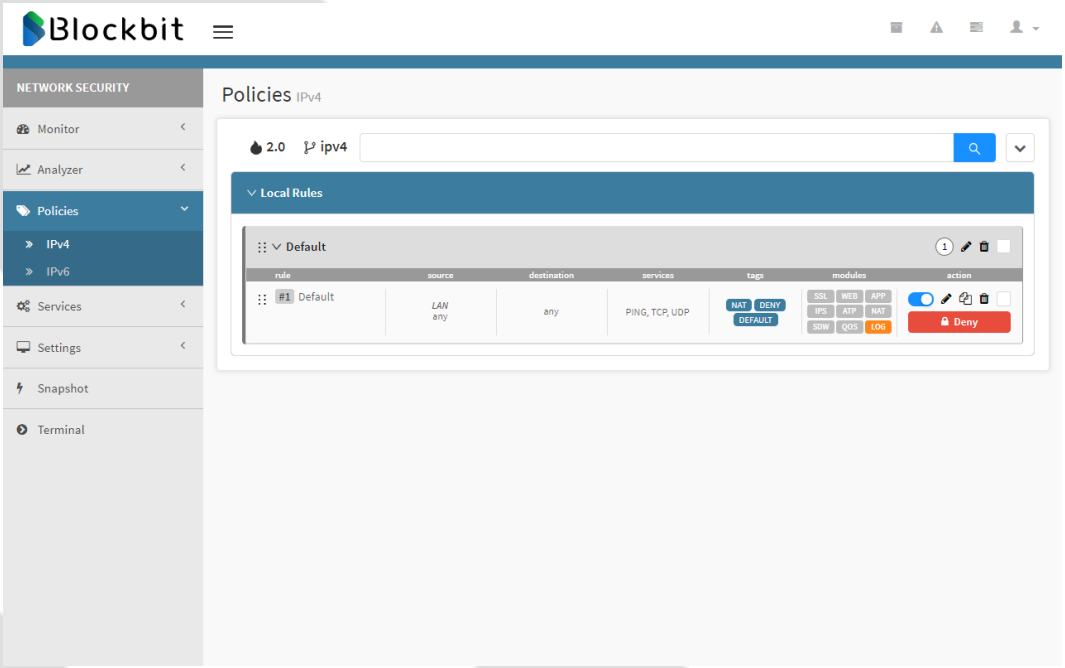
- As políticas de segurança utilizam o método de análise "*FIRST MATCH WINS*".
- As políticas de segurança são cadastradas por "*Agrupamento*", "*Prioridade*" e suportam "*Reordenação*".
- *Classificadas por tipo:*
    - *Protocolo (IPv4 e IPv6)*
    - *Políticas Local*
    - *Políticas GSM - Global Security Management*
- Açoes
    - Permitir
    - Bloquear
    - Rejeitar

2.4.1 Políticas populadas (compliance default)

O Blockbit UTM contempla uma única políticas de segurança pré-configurada, essa políticas visa uma implementação básica para o gerenciamento do tráfego de saída no acesso à internet.

Definida como política "*Default*" de sistema, e populada no modo "*Enable*" com ação padrão de "*Bloqueio*" com o recurso de "*Traffic Log*" no modo "*Enable*".

Clique em [Policies] >> [IPv4].



As Políticas de segurança usam a metodologia de cadastro por agrupamento. Os grupos visam integrar padrões de políticas usando como critério comum o parâmetro "X" ou "Y", para sua aplicabilidade de maneira que defina sua finalidade.

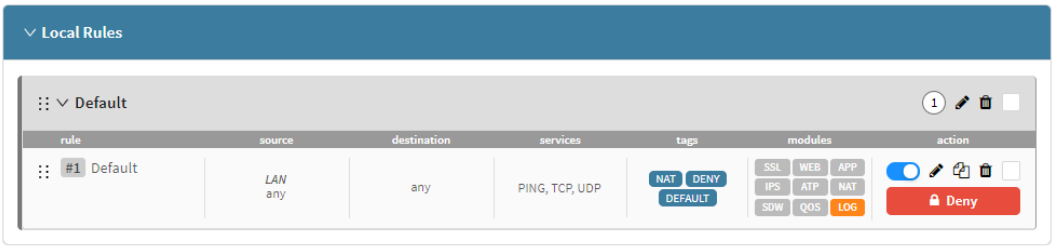
A política default foi populada usando como critério o "*Bloqueio total do tráfego da rede LAN para qualquer destino nos protocolos padrões "TCP/ UDP e PING (ICMP), com a opção de gerar "Log" de todo o tráfego*".

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.

Política 1: Default

Bloqueio total do tráfego com "*Origem*" a rede LAN com "*Destino*" qualquer endereço, e os principais protocolos "*TCP, UDP* e *PING(ICMP)*", com a opção de gerar "*Log*". Todo o tráfego que não se enquadrar em nenhuma política acima, será enquadrada na respectiva política "*Default*".



Vale ressaltar que a implementação desta política visa ÚNICA e EXCLUSIVAMENTE gerar LOG dos ACESSOS não AUTORIZADOS.

2.5 Políticas de segurança I

2.5.1 Definindo grupos de políticas

Vamos exemplificar o cadastro de grupos e alguns exemplos de políticas.

O modelo apresentado visa orientar a modelagem de grupos e políticas baseado no conceito fundamental de ordenação e tratamento das políticas "*Fisrt match Wins*" apresentado em seção anterior.

Antes da criação das políticas, leia atentamente suas descrições, verifique se existem os objetos de "endereço IP", "serviços", "tabela de horários", e os "perfis de inspeção", antes da criação da política e defina-os se necessário.

Lembre-se que os filtros de "Inspeção profunda", são baseados nos perfis configurados nos serviços: "Application Control", "Intrusion Prevention", "Threat Protection" e "Inspeção SSL", aplicados integrados às "Políticas de segurança"., para qualquer modalidade de política: NAT, Forward ou Web.

Definição de grupos:

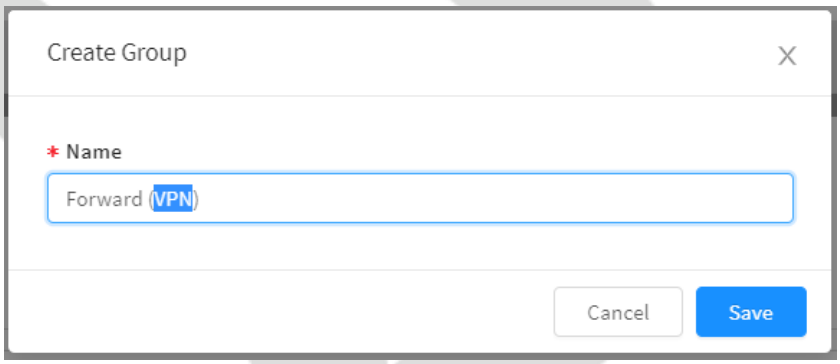
Clique em Create Group [ ] cada um respectivamente.

- Grupo: [Forward]

Finalidade: Definir as políticas para o gerenciamento do tráfego entre as redes/ subredes internas e estendidas. Ex.: "*Rede Local x Rede DMZ*".

Neste grupo vamos definir políticas de "*permissão*" e "*bloqueio*" do tráfego não autorizado, para detecção e geração de "*log*" entre as redes internas e estendidas (DMZ, Vlans).

- Grupo: [Forward (VPN)]



Finalidade: Definir as políticas para o gerenciamento do tráfego das redes estendidas da VPN por meio das interfaces WAN (Internet) para as redes/ subredes internas e DMZ.

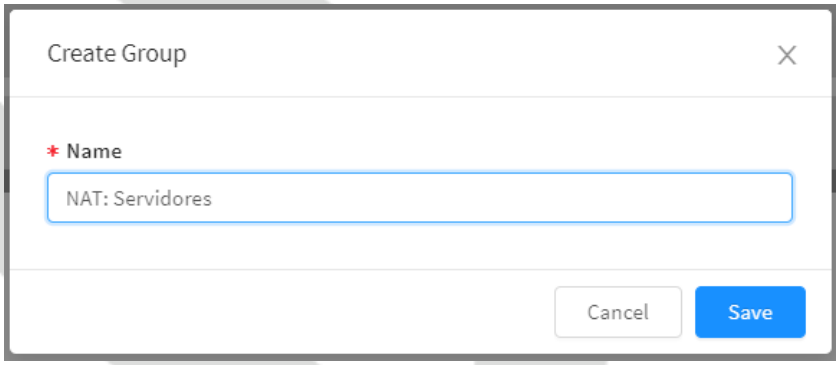
Ex.1.: "*Rede VPN Client x Rede Local Corp*".

Ex.2.: "*Rede VPN Client x Redes VLANs Corp*".

Ex.3: "*Rede VPN Client x Rede DMZ*".

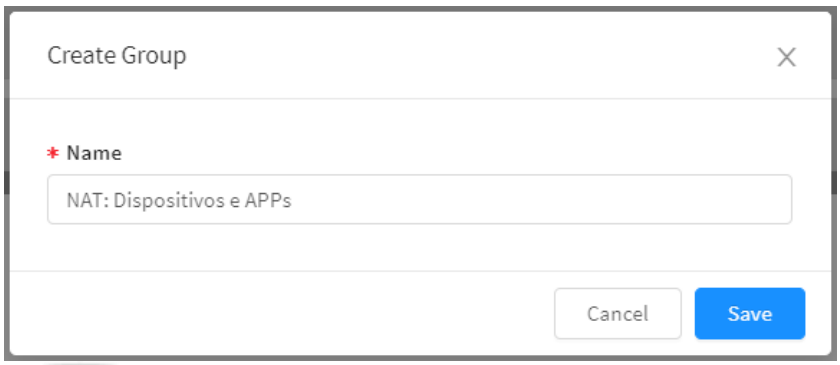
Neste grupo vamos definir políticas de "*Permissão*" e "*GreyList*" para o tráfego autorizado, das redes estendidas VPN Site.B para as redes *(Local Corp; VLANs Corp e Dmz)*.

- Grupo: [NAT: Servidores]



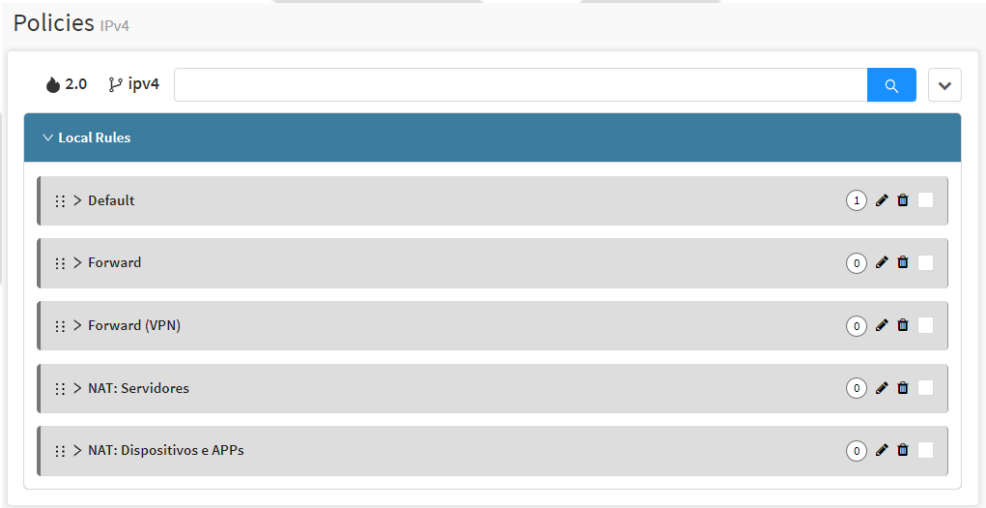
Finalidade: Definir as políticas para o gerenciamento do tráfego dos "*Servidores*" da rede com destino a rede WAN (Internet), no modo "*Mascarado*", ou seja, sem a intervenção de um servidor "*Proxy*".

- Grupo: [NAT: Dispositivos e APPs]



Finalidade: Definir as políticas para o gerenciamento do tráfego de dispositivos da rede, com destino a rede WAN (Internet) para dispositivos da rede como: "Estações de trabalho de usuários específicos", "Smartphones, mobiles" e "Aplicações desktop", no modo "Mascarado", ou seja, sem a intervenção de um servidor "Proxy".

Em ambos grupos de "Mascaramento – [NAT]" a proposta é definirmos políticas de "Permissão" e/ou "GreyList", para permitir o tráfego inicialmente classificado como "confiável", para alguns dispositivos da rede, no entanto, com a condição de "Inspecionar" o tráfego e validar sua legitimidade.



2.5.2 Políticas de Encaminhamento (Forward)

Política de Encaminhamento 1: Rede Local Corp x Rede DMZ

Selecione o grupo [Forward]

Descrição da compliance:

Adicionar uma política de encaminhamento (Forward) entre as redes: "*Local Corp*" e "*DMZ*", para os protocolos TCP, UDP e ICMP.

[Properties]

- → Name = "*Forward Rede local Corp vs Rede DMZ*";
- → Description = "*Forward Rede local Corp vs Rede DMZ*";
- → Action = "*Allow*";
- → Tags = "*DMZ*";
- → Policy Group = Selecione: "*Forward*";
- → Enable: "*[√] Traffic logging*";

[Conection] >>

{Source} → IP Address = Selecione: "*Objeto end.* → *Ex.: Rede Local Corp – IP 10.0.X.0/24*";

{Destination} → IP Address = Selecione: "*Objeto end.* → *Ex.: Rede DMZ – IP 172.16.x.0/24*";

→ Service = Selecione: "TCP, UDP e PING *{ICMP}*";

Clique em Create Policy [ ] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [Save].

Política de Encaminhamento 2: Rede VPN Client x Rede local

Selecione o grupo [NAT: Servidores]

Descrição da compliance:

Adicionar uma política de encaminhamento (Forward) entre as redes: "*VPN Client*" e "*Local*", para os protocolos TCP, UDP e ICMP, com inspeção do tipo IPS Server.

[Properties]

→ Name = "Forward Rede VPN Client vs Rede Local";

→Description = "Forward Rede VPN Client vs Rede Local";

→Action = "Allow";

→ Tags = "VPN";

→ Policy Group = Selecione: "Forward (VPN)";

→ Enable: "[√] Traffic logging";

[Conection] >> {Source}

→ Network Zone = Selecione: "WAN";

→ IP Address = Selecione: "Objeto end. → Ex.: Rede VPN Client – IP 172.19.21.0/24";

[Conection] >> {Destination}

→ IP Address = Selecione: "Objeto end. → Ex.: Rede Local – IP 10.0.X.0/24";

→ Service = Selecione: "TCP, UDP e PING {ICMP}";

[Inspection] >> {Inspection}

→ Enable: [√] SSL Inspection = Selecione: Ex.: "Filtro SSL Inspection Https";

→ Enable: [√] Intrusion Prevention = Selecione: Ex.: "Sensor IPS modo Server";

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

2.5.3 Políticas de Mascaramento (NAT)

Política de Mascaramento 1: Servidor de DNS – Windows AD

Selecione o grupo [NAT: Servidores]

Descrição da compliance:

Adicionar uma política de mascaramento "*NAT (Network Address Translate)*" para o servidor de DNS da rede (Srv Windows AD) com destino ao serviço DNS porta/protocolo (53/UDP).

[Properties]

→Name = "NAT: DNS Recursivo Windows AD";

→Description = "NAT: DNS Recursivo Windows AD";

→Action = "Allow";

→Tags = "NAT", "Servidores";

→Action = "Allow";

→Policy Group: Selecione = "NAT: Servidores";

→Enable: "[√] Traffic logging";

[Conection] >>{Source}

→ IP Address = Selecione: "Objeto end. → Ex.: Srv. Windows AD – IP 192.168.101.245/32";

[Conection] >>{{Destination}

→ Service = Selecione: "DNS";

[Inspection] >>{Inspection}

→ Enable: [√] Intrusion Prevention = Selecione: Ex.: "Sensor IPS modo Server";

[Routing] >> {Gateway}

→ Enable: "[√] [NAT] – Default Gateway {Masked}";

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Política de Mascaramento 2: Estação de trabalho - Aluno

Selecione o grupo [NAT: Dispositivos e APPs]

Descrição da compliance:

Adicionar uma política de mascaramento "*NAT (Network Address Translate)*" para um dispositivo específico da rede no modo autenticado. Permitir o tráfego dos Protocolos TCP; UDP e ICMP.

[Properties]

→Name = "NAT: Estação virtual do Aluno..." ;

→Description = "NAT: Estação virtual do Aluno..." ;

→Action = "Allow" ;

→Tags = "NAT" , "Dispositivos" ;

→Policy Group = Selecione: "[NAT: Dispositivos e APPs]" ;

→ Enable: "[√] Traffic logging" ;

[Conection] >> {Source}

→IP Address = Selecione: "Objeto end. → Ex.: Est. Virtual do Aluno - IP 10.0.X.1/32" ;

[Conection] >> {Destination}

→Service = Selecione: "TCP, UDP e PING {ICMP}" ;

[Conection] >> {Identif...}

→Enable: "[√] Authentication" Selecione: "[√] User [User_Name_Aluno]" ;

[Inspection] >>{Inspection}

→ Enable: [√] SSL Inspection = Selecione: Ex.: "Filtro SSL Inspection Https" ;

→ Enable: [√] Intrusion Prevention = Selecione: Ex.: "Sensor IPS modo Client" ;

→ Enable: [√] Threat Protection = Selecione: Ex.: "Inspeção Anti-APT..." ;

[Routing] >>{Gateway}

→ Enable: "[√] [NAT] – Default Gateway {Masked}" ;

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Política de Mascaramento 3: Servidor de Email – na Amazon

Selecione o grupo [NAT: Dispositivos e APPs]

Descrição da compliance:

Adicionar uma política de mascaramento "*NAT (Network Address Translate)*" para toda a rede local, no modo autenticado, no acesso ao servidor de Email do seu domínio, alocado em um datacenter. Permitir o tráfego dos serviços e protocolos: "*IMAP(143); IMAPs(993); SMTP sub(587) e SMTPs(465)*". Habilitar QoS com prioridade "Alta".

[Properties]

→Name = "NAT: Acesso Srv @Emaill na Amazon";

→Description = "NAT: Acesso Srv @Email na Amazon;

→Action = "Allow";

→Tags = "NAT", 'Dispositivos", "Email", "Nuvem";

→Policy Group = "NAT: Dispositivos e APPs";

→ Enable: "[√] Traffic logging";

[Conection] >> {Source}

→Network Zone = Selecione: "LAN";

[Conection] >> {Destination}

→ IP Address = Selecione: "Objeto end. → Ex.: Srv. @Email Amazon - IP 200.201.202.203/32";

→Service = Selecione: "IMAP, IMAPs, SMTP Subm, SMTPs";

[Conection] >> {Identif...}

→ Enable: "[√] Authentication";

[Routing] >> {Gateway}

→ Enable: "[√] [NAT] – Default Gateway {Masked}";

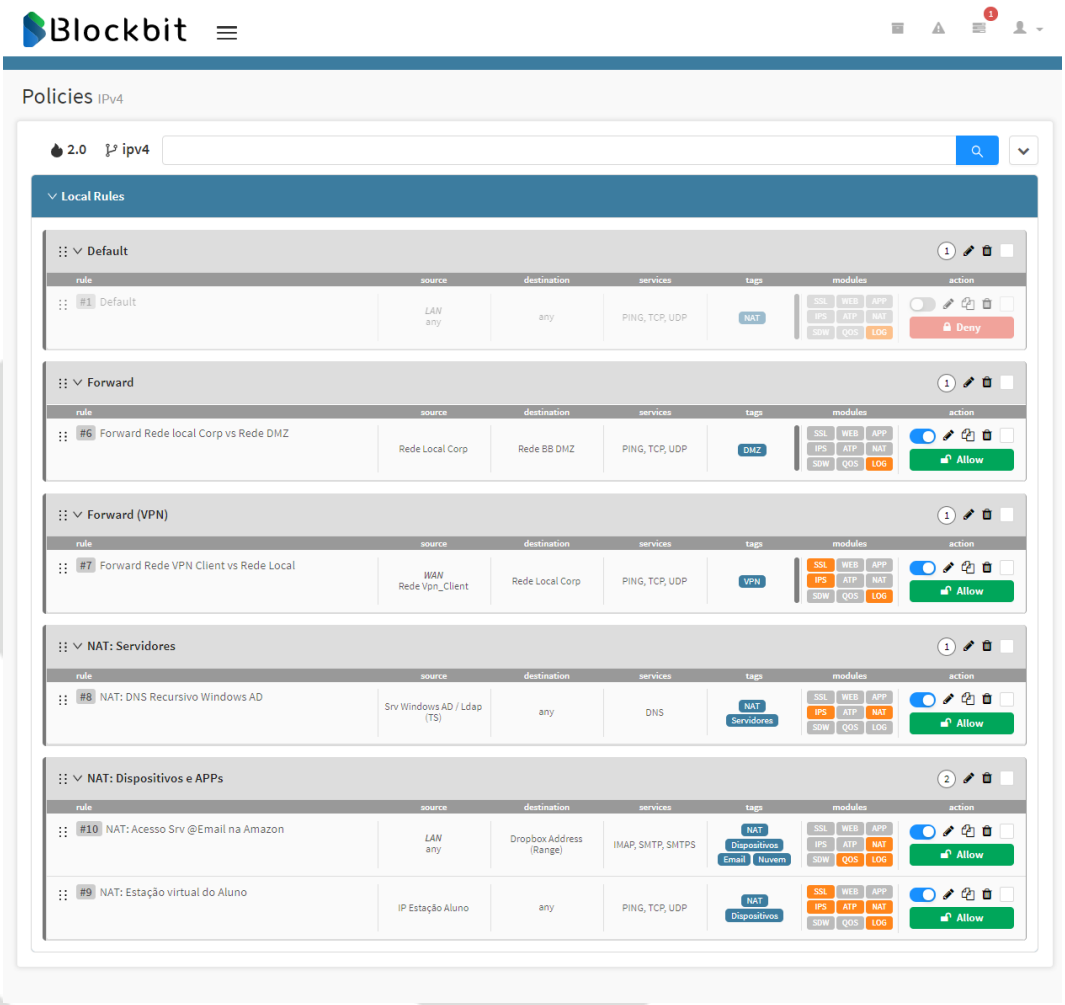
[Routing] >> {QoS}

→ Enable: "[√] Traffic Shaping = Selecione: "Priority = High (Alta)";

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Ao final das configurações das políticas exemplos aplicadas, temos o seguinte resultado:



VERIFIQUE a Ordenação dos “GRUPOS” e “Políticas de segurança.

Esta tarefa é muito importante, e é ela a responsável pelo resultado pretendido pelas definições das políticas de segurança aplicadas. Neste momento o administrador deve verificar de forma individual se cada grupo e política reflete exatamente “ Compliances definidas” .

NÃO se esqueça de APLICAR A *Fila de comandos* [ ]

2.6 Políticas de Segurança II

Pensando no modelo tradicional de definições de políticas, numa estrutura "*Top Down*" as políticas seriam definidas nesta ordem: "*Exceções, seguidas dos Bloqueios, e por fim as Permissões*".

O modelo de configuração de filtros Web integrados a "*Inspeção SSL*", onde definimos no mesmo perfil, as ações de "*Bloqueio*", "*Permissão*" para filtros de "*Categoria Web*", "*Categorias Customizadas*", "*Surf Control*", "App G-Suite" e "SafeSearch", diminui de forma exponencial a quantidade de políticas necessárias para atender conformidades e compliances para assegurar que o tráfego da rede seja legitimo e confiável.

Com um número pequeno de políticas, a capacidade de throughput do seu dispositivo aumenta, maximiza o uso de recursos de CPU e da memória utilizados, sem onerar seu desempenho.

Além de facilitar a análise e gerenciamento das conformidades por meio do monitoramento do tráfego e dos resultados de relatórios e da correlação de eventos, identificados na análise da política unificada.

2.6.1 Definindo grupos de políticas Web Proxy

Vamos exemplificar o cadastro de grupos e alguns exemplos políticas.

O modelo apresentado visa orientar a modelagem de grupos e políticas baseado no conceito fundamental de ordenação e tratamento das políticas "*Fisrt match Wins*" apresentado em seção anterior.

Mencionado na seção anterior , lembre-se que os filtros de "Inspeção profunda", são baseados nos perfis configurados nos serviços: "Application Control", "Intrusion Prevention", "Threat Protection" e "Inspeção SSL", aplicados integrados às "Políticas de segurança"., para qualquer modalidade de política: NAT, Forward ou Web.

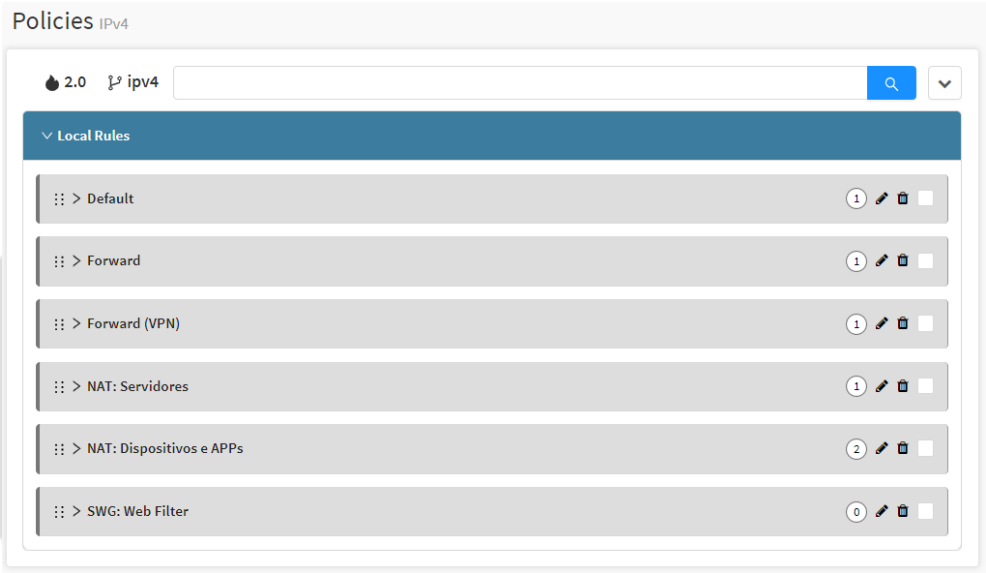
Definição de grupos:

Clique em Create Group [ ] cada um respectivamente.

- Grupo: [WEB Filter: Proxy]

Finalidade: Definir as políticas de gerenciamento do tráfego para a rede WAN (Internet) via "*Proxy*".

Neste grupo vamos definir políticas de "*Permissão*" e de "*GreyList*", ou seja, a fim de permitir o tráfego inicialmente classificado como "*confiável*", no entanto com a condição de "*Inspecionar*" o tráfego para validar a sua legitimidade e aplicar o descarte dos pacotes identificados com conteúdo "*inapropriado ou malicioso*".



2.6.2 Políticas de segurança – Web Proxy

No modelo de políticas de "*Proxy*" não temos a condição de gerenciamento do tráfego por políticas de "*Bloqueio*". A ausência dê política é classificado como tráfego bloqueado, no entanto, sem a geração de log.

A geração do "*Log*" dos acessos não autorizados é aplicada com base na opção "*Traffic Log*" habilitada no tratamento do fluxo de pacotes na política, associada as opções de filtro de "*inspeção*" do tipo "*Web Filter*" que sinaliza se as categorias de url's e outros controles serão permitidos ou negados.

Selecione o grupo [WEB Filter: Proxy]

Política Web 1 - Web Navegação livre

Descrição da compliance:

Vamos adicionar uma política de "*Permissão*" no acesso WEB (Http e Https) para a rede local, no modo autenticado sem inspeção SSL.

[Properties]

→Name = "WEB: Navegação Livre";

→Description = "WEB: Navegação Livre";

→Action = "Allow";

→Tags = "WEB";

→Policy Group = "SWG: Web Filter";

→ Enable: "[√] Traffic logging";

[Conection] >> {Source}

→Network Zone = Selecione: "LAN";

[Conection] >> {Destination}

→Service = Selecione: "HTTP/ HTTPS";

[Conection] >> {Identification}

→ Enable: "[√] Authentication";

[Inspection] >>{Inspection}

→ Enable: [√] Web Filter = Selecione: Ex.: “ Navegação Livre” ;

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Política Web 2 – Categorias Risco de Segurança - depto financeiro

Descrição da compliance:

Adicionar uma política de "*GreyList*" no acesso WEB (Http/Https).

Esta política deve considerar a origem: "*Rede Lan*" com destino aos serviços "*Http* e *Https*", somente para os usuários membros do grupo "*depto financeiro*".

Aplicar os filtros de segurança e inspeção do tipo "*Inspection SSL*", considerar "*SSL by-pass*" o acesso a sites considerados confiáveis para o perfil de atividades do depto financeiro.

Aplicar filtros de inspeção do tipo "*Web Filter*" exemplificado na criação do perfil para bloqueios de URL's de categorias identificadas como "*Risco de segurança e Ética*".

Aplicar Filtros de inspeção do tipo "*APP Control*" exemplificado na criação do perfil para bloqueio dos APP's de Risco e inapropriados para uso no ambiente corporativo.

[Properties]

→Name = "WEB: Depto Financeiro - Bloqueio Categorias de Risco...";

→Description = "WEB: Depto Financeiro - Bloqueio Categorias de Risco...";

→Action = "Allow";

→Tags = "WEB", "Bloqueio_WEB", "G-Suite", "SafeSearch";

→ Policy Group = "SWG: Web Filter";

→ Enable: "[√] Traffic logging";

[Conection] >> {Source}

→Network Zone = Selecione: "LAN";

[Conection] >> {Destination}

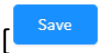
→Services = Selecione: "HTTP/ HTTPS";

[Conection] >> {Identification}

→ Enable: "[√] Authentication – [√] Groups = Selecione: "financeiro";

[Inspection] >>{Inspection}

→ Enable: [√] SSL Inspection = Selecione: Ex.: “Navegação no SSL Inspection”;
→ Enable: [√] Web Filter = Selecione: Ex.: “Categoria de Risco e Ética (Depto Financeiro”;

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Políticas Web 3 – Aplicativos de entretenimento – horário livre

Descrição da compliance:

Adicionar uma política de "*GreyList*" no acesso WEB (Http/Https).

Esta política deve considerar a origem: "*Rede Lan*" com destino aos serviços "*Http* e *Https*", somente para os usuários membros do grupo "*depto financeiro*".

Aplicar os filtros de segurança e inspeção do tipo "*Inspection SSL*", considerar "*SSL by-pass*" o acesso a sites considerados confiáveis para o perfil de atividades do depto financeiro.

Aplicar filtros de inspeção do tipo "*Web Filter*" exemplificado na criação do perfil para bloqueios de URL's de categorias identificadas como "*Risco de segurança* e *Ética*".

Aplicar Filtros de inspeção do tipo "*APP Control*" exemplificado na criação do perfil para permissão dos App's das categorias consideradas de Entretenimento. Ex.: "*Streaming, Social, Games, Mobile*".

[Properties]

→Name = "Web: Navegação hora. entretenimento";

→Description = "Web: Navegação hora. entretenimento";

→Action = "Allow";

→Tags = "Web", "APP Control";

→Policy Group = "SWG: Web Filter";

→ Enable: "[√] Traffic logging";

[Conection] >>{Source}

→Network Zone = Selecione: "LAN";

[Conection] >>{{Destination}

→Service = Selecione: "HTTP/ HTTPS";

[Conection] >> {Identification}

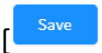
→ Enable: "[√] Authentication – [√] Groups = Selecione: "financeiro";

[Inspection] >>{Inspection}

→ Enable: [√] SSL Inspection = Selecione: Ex.: “Navegação no SSL Inspection”;

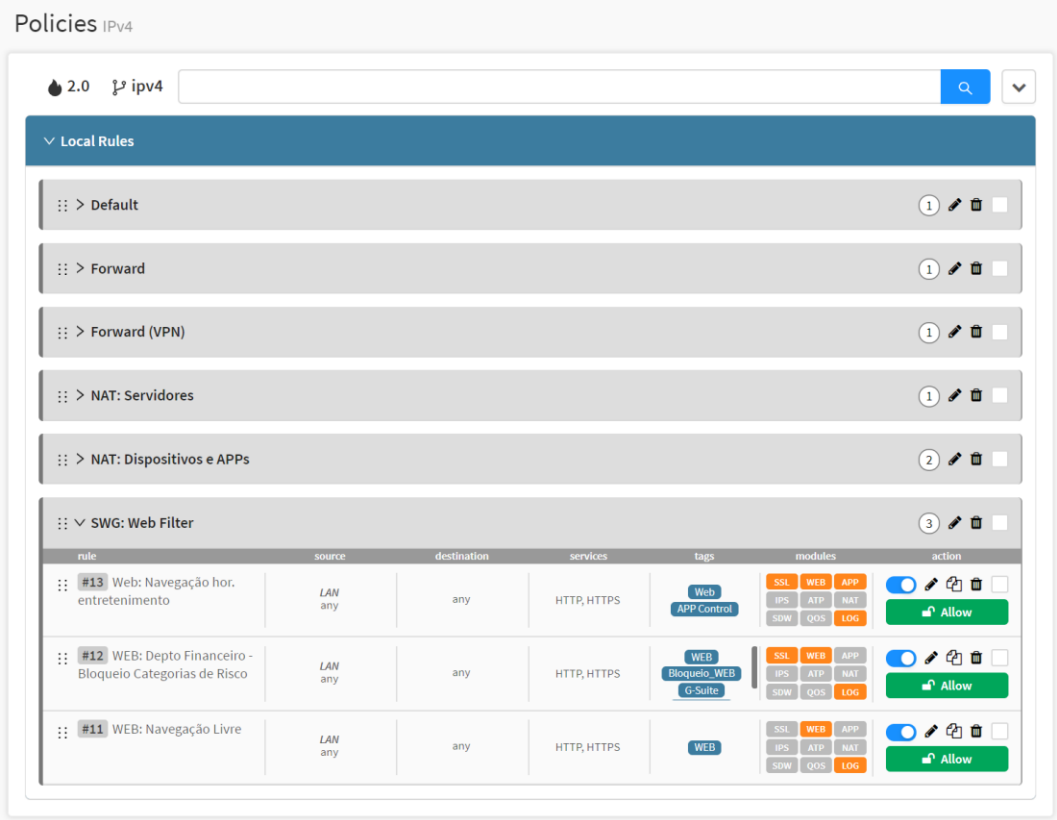
→Enable: [√] App Control = Selecione: Ex.: “Controle de Apps – Hor. Entretenimento”;

→ Enable: [√] Web Filter = Selecione: Ex.: “Categoria de Risco e Ética (Depto Financeiro”;

Clique em Create Policy [] e configure cada aba de acordo com as definições da política aplicada. Depois clique em [

].

Ao final das configurações das políticas exemplificadas para o exercício, temos o seguinte resultado:



VERIFIQUE a Ordenação dos “GRUPOS” e “Políticas de segurança.

Esta tarefa é muito importante, e é ela a responsável pelo resultado pretendido pelas definições das políticas de segurança aplicadas. Neste momento o administrador deve verificar de forma individual se cada grupo e política reflete exatamente as “*Compliances definidas*”.

NÃO se esqueça de APLICAR A *Fila de comandos* [ ]

Dicas antes de APLICAR os TESTES de funcionalidade sobre as políticas SWG exemplificadas acima:

1. Alterar a política de NAT do dispositivo do aluno, para "*Permitir*" somente o tráfego do protocolo DNS;
2. Se julgar necessário, reordene as políticas de Proxy SWG recém configuradas:
3. Mantenha "*Habilitada*" a política "*[Web: Navegação Livre]*";
4. *Desabilite as demais políticas WEB*
5. *Realize os testes de navegação;*
6. *Monitore* o "Firewall" e o "Proxy";

   >> Monitor >> Live sessions >> na aba [Connections]

   [Frewall]; [new cnxs;] e/ou

   >> Monitor >> Live sessions >> na aba [Connections]

   [Web Proxy]"; [new cnxs]

7. *Habilite as próximas políticas, "Uma por vez" e reaplique os testes de navegação {itens 5, 6 e 7}.*


Blockbit
it's easy to be secure