

Manual TRAFip

Manual TRAFip

Índice

| | |
|--|----|
| Prefácio | x |
| Público alvo | x |
| Convenções utilizadas neste manual | x |
| 1. Introdução | 1 |
| Sobre | 1 |
| Principais recursos | 1 |
| Requisitos mínimos | 2 |
| Hardware | 2 |
| Navegador | 2 |
| 2. Conceitos básicos | 3 |
| Netflow | 3 |
| jFlow | 3 |
| IPFIX | 3 |
| Huawei Netstream | 3 |
| sFlow | 4 |
| Definições dos objetos | 4 |
| Análise de cenários no TRAFip | 4 |
| Redes full mesh | 4 |
| Redes ponto-multiponto | 5 |
| Redes de provedores de serviço de internet | 6 |
| 3. Guia rápido de inicialização | 8 |
| Acessando a interface web | 8 |
| Análise de tráfego de interfaces | 9 |
| 4. Gerador de gráfico Telcomanager | 10 |
| Período | 10 |
| Gráfico diário | 10 |
| Gráfico semanal | 10 |
| Gráfico mensal | 10 |
| Gráfico trimestral | 10 |
| Gráfico anual | 10 |
| Gráfico bienal | 11 |
| Gráfico de cinco anos | 11 |
| Gráfico customizado | 11 |
| Recursos | 11 |
| Caixa de estatísticas | 11 |
| Mostrar valor | 11 |
| Zoom vertical | 11 |
| Uma curva | 11 |
| Modo relativo | 11 |
| Configuração de eixos | 12 |
| Associar a Graph Set | 12 |
| Salvar imagem | 12 |
| Tipo de gráfico | 12 |
| Gráfico agregado | 12 |
| Aproximar e afastar | 12 |
| Exportar | 12 |
| Atualização automática | 13 |
| Relatório | 13 |
| Teclas | 13 |
| 5. Dados históricos | 15 |
| Resumo da rede | 15 |

| | |
|---|----|
| Favoritos | 16 |
| Adicionando objetos aos favoritos | 16 |
| Removendo objetos dos favoritos | 16 |
| Totais | 16 |
| Subredes | 16 |
| Definições | 16 |
| Configuração | 16 |
| Importar arquivos de subredes | 17 |
| Grupo de subredes | 18 |
| Definições | 18 |
| Configuração | 18 |
| Agrupamento | 18 |
| Dispositivos | 19 |
| Criando um dispositivo utilizando o Assistente | 22 |
| Verificando objetos mapeados para o dispositivo | 23 |
| Importar arquivos de dispositivo | 23 |
| Grupos de interface | 24 |
| Tráfego não mapeado | 25 |
| Aplicações | 25 |
| Classificação | 26 |
| Importar arquivos de aplicação | 26 |
| Grupos de aplicação | 27 |
| Protocolos | 27 |
| Importar arquivos de protocolos | 27 |
| Sistemas autônomos | 28 |
| Importar arquivos de sistemas autônomos | 28 |
| Grupo de sistema autônomo | 29 |
| Tipo de serviço | 29 |
| Importar arquivos ToS | 30 |
| Grupo de ToS | 30 |
| Relatórios | 31 |
| | 31 |
| Templates | 31 |
| Tráfego Suspeito | 32 |
| Top N | 33 |
| Perfil de tráfego | 34 |
| Syslog | 35 |
| Dados brutos | 36 |
| Relatório de Projeção | 38 |
| Graph set | 40 |
| Definições | 40 |
| Criação | 40 |
| Adicionando gráficos | 40 |
| Visualizando um graph set | 41 |
| Editando um graph set | 41 |
| Gerando gráficos para um graph set | 41 |
| NOC Display | 41 |
| 6. Configuração | 42 |
| Perfis de tráfego | 42 |
| Definições | 42 |
| Configuração | 42 |
| Tipos de análises | 43 |
| Domínios | 44 |
| Definições | 44 |

| | |
|--|----|
| Configuração | 44 |
| Interfaces RFI | 45 |
| Coletoras | 46 |
| Importando arquivos de coletoras | 47 |
| Objetos | 47 |
| Importando arquivos de objetos | 47 |
| Mapeadores | 48 |
| Mapeamento cruzado de OIDs | 49 |
| Associando dispositivos aos mapeadores | 49 |
| Exportando e importando mapeadores | 49 |
| EPM (Extended Processing Module) | 49 |
| Regras | 50 |
| Criação de regras | 50 |
| Filtro 'No Response' | 50 |
| Credencial de dispositivo | 51 |
| 7. Ferramentas | 52 |
| Software externo | 52 |
| Telcomanager Windows Collector | 52 |
| Telcomanager Host Agent | 52 |
| | 52 |
| Discovery | 52 |
| 8. Sistema | 53 |
| Registro de acesso | 53 |
| Acesso de usuário | 53 |
| Acesso simultâneo | 53 |
| Backup/Restore | 53 |
| Backup local de configuração | 53 |
| Restore local de configuração | 53 |
| Backup remoto | 53 |
| Restore remoto | 54 |
| Situação da restauração | 54 |
| Parâmetros | 54 |
| Active directory | 54 |
| Agentes de associação | 55 |
| Análise de ameaças | 55 |
| Armazenamento de dados | 56 |
| Arquitetura distribuída | 57 |
| Aviso de Expiração | 58 |
| Backup | 58 |
| Cisco WAAS | 58 |
| Configuração de HTTPS | 58 |
| Configuração do agente de captura | 59 |
| Configuração regional | 59 |
| EPM | 59 |
| Filtro simples | 59 |
| Grafador | 60 |
| Histórico de configuração | 60 |
| Integridade de segurança | 61 |
| Login automático | 61 |
| Logotipo | 61 |
| Mapeador de objetos | 61 |
| Nível de log | 62 |
| Personalização de interface | 62 |
| Preferências locais | 62 |

| | |
|--|----|
| Projeção | 63 |
| Redirecionamento de login | 63 |
| Redundância | 63 |
| Registros de acesso de usuários | 63 |
| Relatórios | 64 |
| Servidor SMS | 64 |
| SMTP | 65 |
| SNMP | 66 |
| TACACS | 67 |
| Tema | 67 |
| TRAFip | 67 |
| Transferência de arquivos | 67 |
| Verificação de exportadores de fluxo | 68 |
| Verificação de versão do sistema | 68 |
| Web Services | 68 |
| Usuários | 68 |
| Editando usuários | 69 |
| Grupos de usuários | 70 |
| Perfis de usuários | 70 |
| Alarme Console | 71 |
| Diagnósticos | 71 |
| Informações de rede | 71 |
| Testes de conectividade | 71 |
| Captura de pacotes | 71 |
| Objetos | 72 |
| Estatísticas de fluxo | 72 |
| Sumarizador | 72 |
| Uso de disco | 72 |
| Arquivos de Log | 73 |
| Logs de configuração | 73 |
| Estatística de Tráfego Suspeito | 74 |
| Fuso horário | 74 |
| Suporte | 74 |
| Sobre | 74 |
| 9. ALARMmanager | 75 |
| Relatórios | 75 |
| Relatórios suprimidos | 75 |
| Relatórios consolidados | 75 |
| Template de Email | 76 |
| Introdução | 76 |
| Customizando o e-mail | 76 |
| Níveis de urgência de alarme | 77 |
| Mudando o nível de prioridade da urgência | 77 |
| Adicionando um novo nível de urgência | 77 |
| Alarmes | 78 |
| Configuração de alarmes padrão | 78 |
| Configuração do alarme de mudança de comportamento | 80 |
| Ações | 83 |
| Gerenciamento de supressão de alarmes | 84 |
| Configuração de perfil de alarme | 85 |
| Alarmes de serviço | 85 |
| Introdução | 85 |
| Fórmula | 85 |
| Console | 85 |

| | |
|--|----|
| Introdução | 85 |
| Operação de Console | 86 |
| 10. Recursos habilitados com licença | 89 |
| Redundância | 89 |
| Conceitos | 89 |
| Habilitando a redundância | 89 |
| Arquitetura distribuída | 90 |
| Conceitos | 90 |
| Pré-requisitos | 90 |
| Implantação | 90 |

Lista de Tabelas

| | |
|--|----|
| 1. Convenções do manual | x |
| 4.1. Teclas | 13 |
| 5.1. Tabela de ícones | 16 |
| 5.2. Formulário de nova subrede | 17 |
| 5.3. Campos de um arquivo de subrede | 17 |
| 5.4. Formulário de grupo de subredes | 18 |
| 5.5. Novo formulário de agrupamento | 19 |
| 5.6. Formulário de novo dispositivo | 19 |
| 5.7. Campos do arquivo de dispositivo | 23 |
| 5.8. Formulário de grupos de interface | 24 |
| 5.9. Formulário de aplicação | 25 |
| 5.10. Campos de arquivo de aplicação | 26 |
| 5.11. Formulário de grupo de aplicações | 27 |
| 5.12. Formulário de protocolo | 27 |
| 5.13. Campos do arquivo de protocolo | 28 |
| 5.14. Formulário de sistemas autônomos | 28 |
| 5.15. Campos de um arquivo de sistema autônomo | 29 |
| 5.16. Formulário de grupo de sistemas autônomos | 29 |
| 5.17. Formulário de ToS | 30 |
| 5.18. Campos dos arquivos ToS | 30 |
| 5.19. Formulário de grupo de ToS | 30 |
| 5.20. Forma do template | 31 |
| 5.21. Relatório de Tráfego Suspeito | 33 |
| 5.22. Relatório Top N | 33 |
| 5.23. Relatório de perfil de tráfego | 35 |
| 5.24. Relatório Syslog | 36 |
| 5.25. Relatório de dados brutos | 37 |
| 5.26. Formulário de configuração de projeção | 38 |
| 5.27. Formulário de relatório de projeção | 39 |
| 5.28. Criação de graph set | 40 |
| 6.1. Formulário de perfil de tráfego | 42 |
| 6.2. Formulário de Domínio | 44 |
| 6.3. Formulário de coletoras | 46 |
| 6.4. Campos de arquivos de coletoras | 47 |
| 6.5. Formulário de Mapeador | 48 |
| 6.6. Perfil automático de regras | 50 |
| 6.7. Formulário de Credencial de dispositivo | 51 |
| 8.1. Formulário de backup remoto | 54 |
| 8.2. Formulário de Active directory | 55 |
| 8.3. Formulário de agente de associação automática de mapeadores | 55 |
| 8.4. Formulário de parâmetros da Análise de ameaças | 55 |
| 8.5. Formulário de armazenamento de dados | 56 |
| 8.6. Formulário dos parâmetros da arquitetura distribuída | 57 |
| 8.7. Formulário de aviso de expiração | 58 |
| 8.8. Formulário de Cisco WAAS | 58 |
| 8.9. Formulário de HTTPS | 59 |
| 8.10. Formulário de configuração do agente de captura | 59 |
| 8.11. Formulário de configuração regional | 59 |
| 8.12. Formulário EPM | 59 |
| 8.13. Formulário de parâmetros do grafador | 60 |
| 8.14. Parâmetros de históricos de configuração | 60 |

| | |
|---|----|
| 8.15. Integridade de Segurança | 61 |
| 8.16. Formulário de configuração de parâmetros de mapeador de objetos | 61 |
| 8.17. Fórmula de nome de dispositivo | 62 |
| 8.18. Formulário de preferências locais | 62 |
| 8.19. Configurações de redundância | 63 |
| 8.20. Formulário de registros de acesso de usuários | 63 |
| 8.21. Dados brutos do TRAFip | 64 |
| 8.22. Formulário de configuração dos relatórios agendados | 64 |
| 8.23. Formulário de servidor SMPP | 64 |
| 8.24. Formulário de parâmetros SMTP | 65 |
| 8.25. Campos de TRAP | 66 |
| 8.26. Configuração do tema | 67 |
| 8.27. Formulário de API de configurações | 68 |
| 8.28. TRAFip's raw data form | 68 |
| 8.29. Formulário de usuário | 69 |
| 8.30. Formulário de usuário | 70 |
| 8.31. Formulário de usuário | 70 |
| 8.32. Colunas ALARMmanager console | 71 |
| 8.33. Captura de pacotes | 72 |
| 9.1. Formulário de relatório de alarmes suprimidos | 75 |
| 9.2. Formulário de alarmes consolidados | 75 |
| 9.3. Template de Email | 76 |
| 9.4. Variáveis de e-mail | 76 |
| 9.5. Formulário de nível de urgência de alarme | 77 |
| 9.6. Formulário de alarme padrão | 78 |
| 9.7. Representação das métricas | 80 |
| 9.8. Formulário de alarme histórico | 80 |
| 9.9. Representação de métricas | 82 |
| 9.10. Formulário de perfil de alarme | 85 |
| 9.11. ALARMmanager console | 86 |

Prefácio

Público alvo

Este manual é designado aos administradores de rede, consultores de rede e parceiros da Telcomanager.

Para entender completamente este manual, o leitor deve ter conhecimento intermediário sobre gerenciamento de redes, protocolo TCP/IP e protocolo SNMP.

Convenções utilizadas neste manual

Este documento utiliza as seguintes convenções:

Tabela 1. Convenções do manual

| Item | Convenções |
|-----------------------------------|--------------------------------------|
| Selecionando um item do menu | Menu → Submenu → Item do menu |
| Comandos, botões e palavras-chave | Fonte em negrito |

Capítulo 1. Introdução

Sobre

TRAFip é um sistema de caracterização de tráfego para redes IP. É implantado na rede de uma forma não intrusiva e recebe informações sobre tráfego IP usando o protocolo Netflow ou pela captura direta em uma das interfaces da rede.

Principais recursos

- Suporte para NetFlow, jFlow, sFlow, IPFIX e Huawei netstream.
- Acesso a todos os recursos do sistema através de um web browser.
- Captura e relatório de Syslog.
- Criação de fórmulas, permitindo que o usuário defina suas próprias KPIs (Key Performance Indicators).
- Arquitetura escalável. O sistema pode crescer no número de elementos coletados pelo uso de appliances coletores remotos e no número de usuários e relatórios suportados pelo meio da implantação de EPMs (Expanded Processing Modules), que são appliances responsáveis por realizar o compartilhamento de carga com o sistema central.
- Alta disponibilidade pode ser oferecida pelo uso de soluções redundantes, em que dois appliances trabalham em HOT-STANDBY.
- Relatórios de projeção.
- Todos os relatórios podem ser salvos como templates, agendados e exportados em formato PDF, HTML e CSV.
- Exportação de imagem de gráfico em massa.
- Flexibilidade na criação de gráficos.
- Gráfico em HTML5 interativo, com recursos como zoom vertical e horizontal, auto-escala e gráficos agregados.
- Banco de dados de alta performance para dados históricos armazenados.
- Relatórios Top N para todos os elementos monitorados.
- Classificação de tráfego em subredes, grupos de subredes, aplicações, dispositivos, protocolos, sistemas autônomos e ToS (Type of Service).
- Perfis de tráfego permitindo o usuário a agrupar objetos do mesmo tipo e depois usar o perfil para classificar o tráfego de qualquer objeto do sistema. Por exemplo, um perfil de tráfego contendo subredes de uma rede podem ser criados e depois associados a cada subrede para produzir gráficos exibindo o tráfego trocado entre elas.
- Filtros RFI (Repeated Flow Interface), que irão filtrar tráfegos repetidos exportados pelos roteadores.
- Captura de tráfego direto na interface de rede do appliance, para ser usado em ambientes onde Netflow ou outro protocolo de fluxo não estão disponíveis.

Requisitos mínimos

Estes requisitos são para os computadores que irão acessar o sistema pelo web browser.

Hardware

- Processador Pentium 2 400 MHZ ou superior.
- 128 MB de memória RAM.

Navegador

- Internet explorer 9+.
- Chrome 4.0+.
- Firefox 7.0+.

Capítulo 2. Conceitos básicos

Netflow

O modo mais escalável para analisar tráfego IP é através do uso do protocolo Netflow, desenvolvido pela Cisco Systems, ou outro protocolo de exportação de fluxo.

No Netflow, os roteadores exportam pacotes UDP contendo informações sobre todo tráfego que passou por eles.

O TRAFip permite a captura deste tráfego e usa a informação para qualificar o tráfego de diferentes maneiras.

Cada pacote UDP pode ter até 1500 bytes de tamanho e carregar informação de até 50 fluxos.

Um fluxo é definido como um tráfego unidirecional contendo 7 chaves: endereço de IP de origem, endereço de IP de destino, porta TCP/UDP de origem, porta TCP/UDP de destino, protocolo de nível 3, byte de ToS e índice de entrada de interface lógica.

É importante salientar que, para ter total visibilidade do tráfego que está passando por um roteador, é recomendado habilitar o NetFlow em todas as suas interfaces.

jFlow

J-Flow é uma implementação de monitoramento de tráfego da Juniper. Essa ferramenta permite que dispositivos da rede colem dados do tráfego e exportem essa informação para as coletoras.

Essa ferramenta de monitoração também é usada como uma técnica de gravação de tráfego. Cada pacote que passa por uma rede é monitorado e as tendências de fluxo da rede são salvas. Depois disso, toda informação gravada é comparada e, dessa forma, é possível que uma anomalia seja detectada.

IPFIX

IPFIX é um modelo proposto pela Internet Engineering Task Force (IETF).

Internet Protocol Flow Information eXport (IPFIX) é um protocolo unidirecional para exportação de dados e é baseado no formato de exportação do NetFlow v9.

A maior vantagem do IPFIX é seu suporte para campos com comprimentos variáveis. Essa funcionalidade é muito útil caso você precise exportar URLs.

Esse protocolo destina-se, principalmente, à exportação de tráfego com alta taxa de fluxo e à aplicação em roteadores de alta velocidade.

Huawei Netstream

NetStream é uma tecnologia de que fornece estatísticas de análise de tráfego desenvolvida pela Huawei Technologies.

Ele é muito similar ao NetFlow: uma vez que um sistema de gerenciamento de rede possui o software NetStream instalado, ele receberá estatísticas do tráfego e do uso de recursos, que foram coletadas pelo NetStream.

sFlow

sFlow é uma tecnologia desenvolvida pela InMon.

Ao contrário das outras ferramentas de monitoramento antes abordadas (NetFlow, J-Flow, IPFIX e NetStream), que são mais utilizadas em roteadores, sFlow é mais popular em switches.

A maior diferença entre o sFlow e o NetFlow é que, enquanto o NetFlow coleta todos os pacotes, o sFlow pega amostras (samples).

Essa característica torna possível saber qual é a tendência da rede e isso acarreta na geração de menos tráfego.

Definições dos objetos

Os objetos abaixo podem ser configurados de forma a classificar o tráfego.

Objetos do TRAFip

| | |
|-----------------------|--|
| Subrede | Bloco de rede IP. |
| Grupos de subrede | Grupos de subrede. |
| Dispositivo | Elementos de rede de exportação de fluxo. Geralmente roteadores. |
| Interfaces | Interfaces lógicas de dispositivos. |
| Grupos de interfaces | Grupos de interfaces. |
| Aplicação | Definição de portas TCP/UDP |
| Protocolo | Número do protocolo da camada de transporte TCP/IP |
| AS (Sistema autônomo) | Número de AS |
| Grupos de AS | Grupos de AS |
| ToS (Tipo de Serviço) | Número de ToS |
| Grupos de ToS | Grupos de ToS |

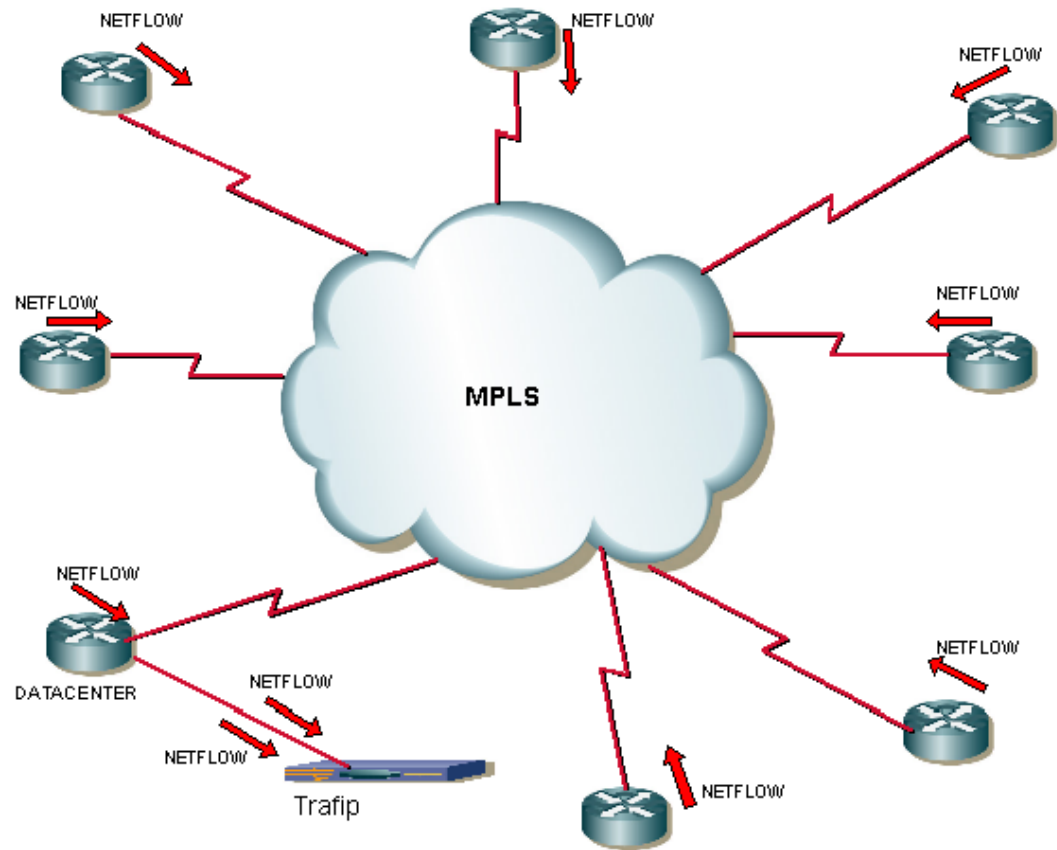
Análise de cenários no TRAFip

Redes full mesh

O TRAFip deve ser posicionado o mais perto possível do roteador que lida com a maior quantidade de tráfego, para que não exista fluxo de tráfego desnecessário através da rede.

Para ter todo o tráfego analisado, é recomendado que todos os roteadores exportem tráfego em todas as interfaces.

A imagem abaixo ilustra todos os roteadores de rede MPLS exportando fluxo para o TRAFip.

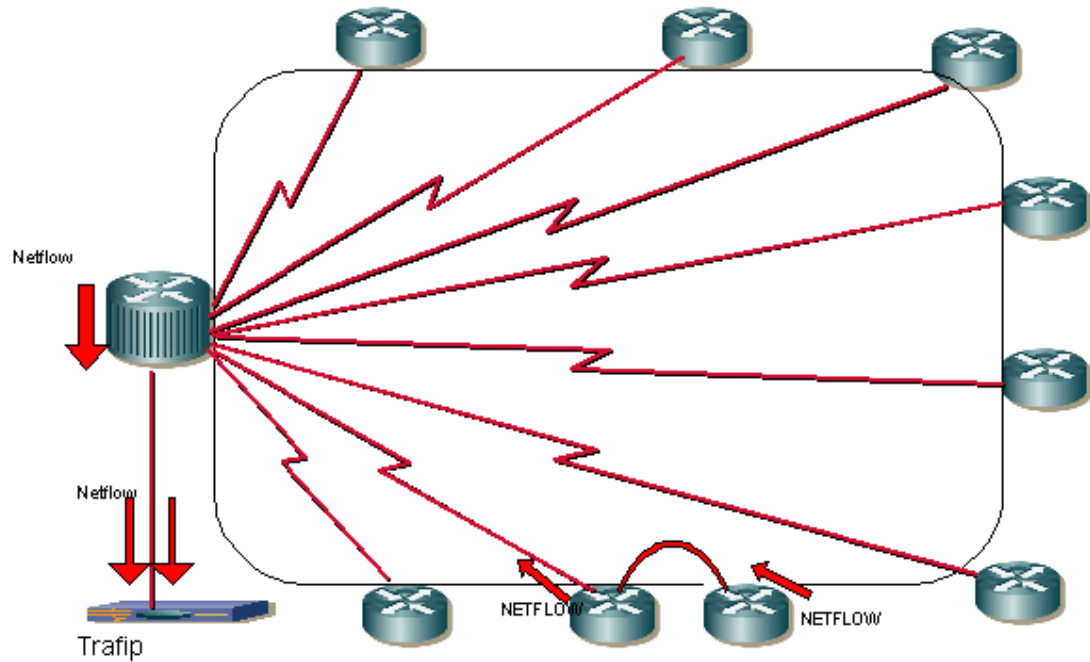


Exemplo de rede full mesh

Redes ponto-multiponto

Neste caso, o TRAFIP deve ser posicionado o mais próximo possível do roteador central.

Uma vez que todo tráfego passa pelo roteador central, é apenas necessário habilitar fluxo de exportação nos roteadores da borda, exceto quando existe tráfego fluindo entre dois roteadores de borda, como ilustrado a seguir.



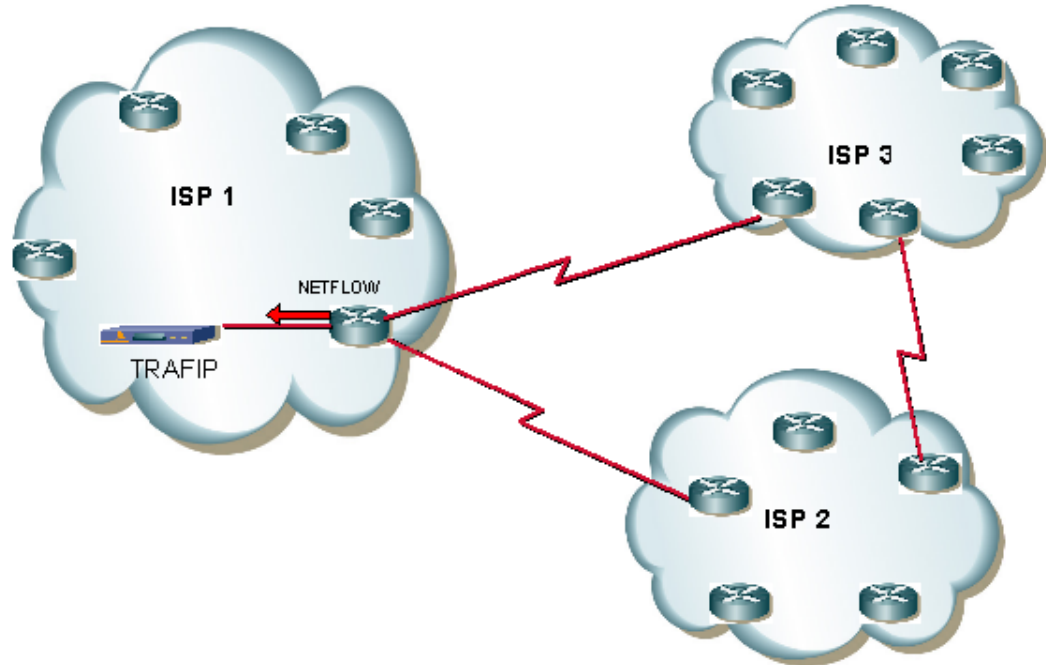
Exemplo de rede ponto-multiponto

Redes de provedores de serviço de internet

Neste ambiente, o TRAFip deve ser posicionado o mais próximo possível do roteador que encaminha a maior quantidade de tráfego.

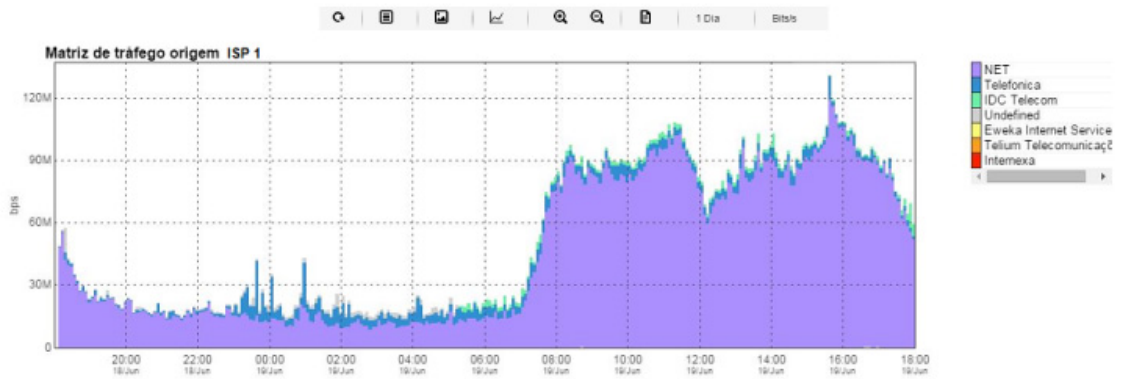
O TRAFip pode ser utilizado para analisar troca de tráfego entre este ISP e outros com o objeto AS (Autonomous Systems). Isto irá ajudar os administradores de rede a melhorar as políticas de troca de tráfego.

A imagem abaixo ilustra este cenário.



Exemplo de rede ISP

O gráfico abaixo é um exemplo de qualificação de tráfego AS, mostrando o quanto do tráfego que está fluindo para fora do ISP1 está sendo encaminhado para cada ISP, representado pelas curvas dos gráficos.



Exemplo de gráfico de um sistema autônomo

Capítulo 3. Guia rápido de inicialização

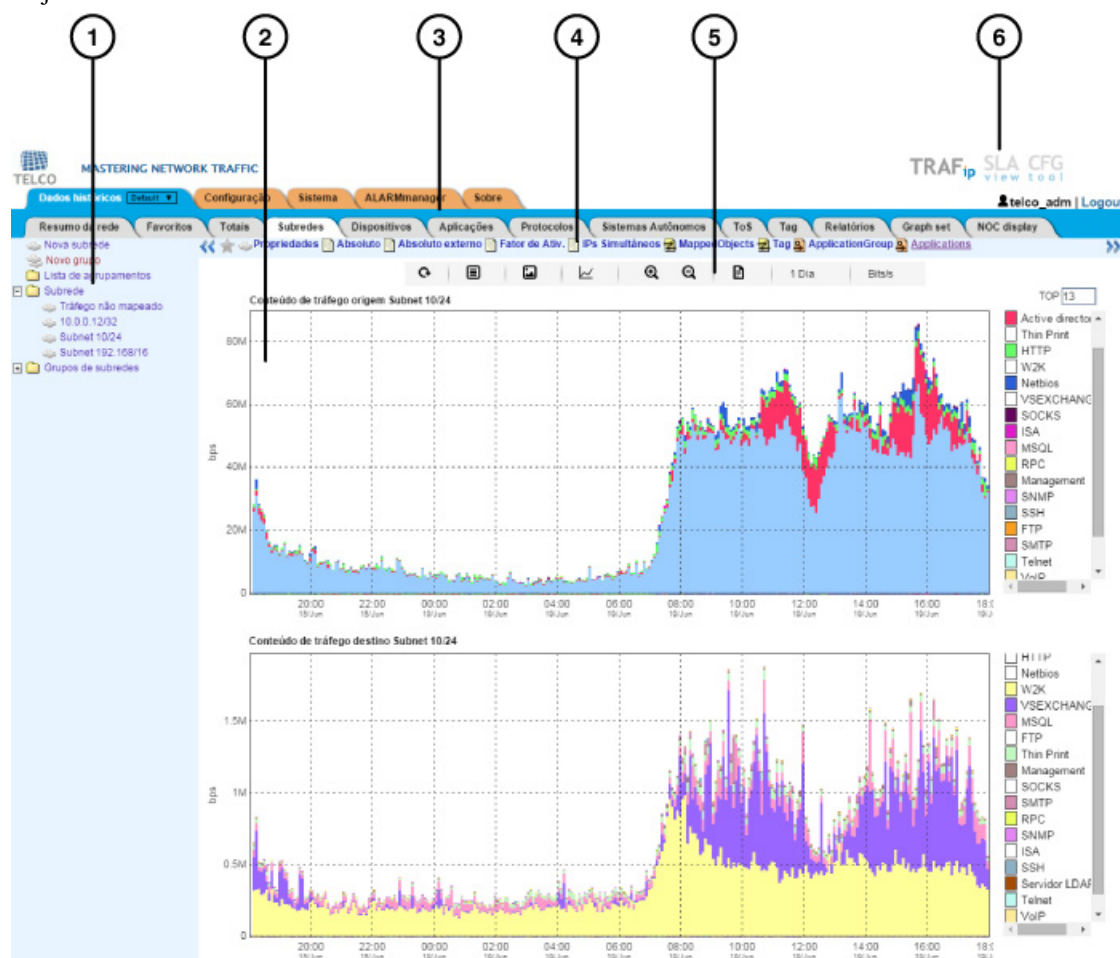
Acessando a interface web

Uma vez que o servidor do TRAFip é acessado digitando seu endereço IP no navegador, escolha o sistema TRAFip clicando no ícone do TRAFip localizado no canto direito superior da janela.

O acesso inicial no sistema pode ser feito utilizando o usuário **telco_admin** e a senha **sysoper**. Neste ponto, é recomendada uma mudança de senha.

Se a autenticação for bem sucedida, uma tela semelhante a que encontra-se abaixo é mostrada ao usuário.

A sessão pode ser encerrada a qualquer momento clicando no ícone de **Logout** no canto direito superior da janela.



Tela principal do TRAFip

A tela principal do sistema é dividida nas seguintes áreas:

Área 1: Menu árvore. Usada para navegar pelos objetos do sistema e configuração dos itens.

Área 2: Display de dados. Usado para mostrar gráficos, relatórios e formas de configuração.

Área 3: Menu principal. Usado para selecionar todos os recursos do sistema.

Área 4: Seleção de gráfico. Usado para selecionar gráficos e propriedades dos objetos.

Área 5: Painel de controle. Usado para acessar as ferramentas dos gráficos.

Área 6: Cabeçalho. Usado para indicar qual usuário está logado, qual está deslogado e trocar entre os sistemas TRAFip e SLAview.

Análise de tráfego de interfaces

Uma vez que os roteadores estão exportando fluxo para o TRAFip, você poderá configurar dispositivos no sistema e realizar uma análise de fluxo nas interfaces de acordo com o seguinte procedimento:

1. Tenha certeza de que há conexão entre todos os elementos de rede que estão exportando NetFlow e o appliance do TRAFip na porta UDP 161 (para tráfego SNMP), 63636 (para exportação de NetFlow) e 6343 (para exportação de sFlow).
2. Aguarde em torno de 5 minutos depois da configuração do roteador e acesse **Sistema** → **Diagnósticos** → **Exportadores de fluxo** .
3. Clique no botão **Editar**, que está próximo aos roteadores identificados e preencha o formulário:
 - a. Modifique os campos **Nome** e **Endereço IP de gerência**. O segundo deve ser um endereço de IP que o roteador possa receber consultas SNMP.
 - b. Preencha a **Versão SNMP** e a **Community** de acordo com as configurações do roteador. Em seguida, com o campo (Configuração de sampling rate) em modo Manual, insira o valor 1 no campo **Netflow sampling rate**.
 - c. No campo **Mapeadores**, selecione **Interface**. Com isso, as interfaces dos roteadores serão descobertas.
4. Espere 5 minutos para que o sistema possa mapear as interfaces do roteador e acesse **Dados históricos** → **Dispositivos** → **Grupos de Interface** . Depois clique no botão Novo e preencha a configuração de grupos de interface da forma:
 - a. Preencha o campo **Nome**.
 - b. No campo **Interfaces**, use o carácter * para filtrar as interfaces desejadas.
 - c. Nas caixas de seleção de **Perfil**, selecione **Perfis de conteúdo** na guia e depois selecione **Protocolos** e **Aplicações**.
5. Aguarde em torno de 10 minutos, depois acesse a interface de grupo criada e clique no ícone gráfico **Aplicações** na área de navegação do gráfico para verificar as aplicações classificadas no tráfego do grupo de interface.
6. Clique com o botão direito do mouse na área do gráfico e selecione a opção **Gerar Relatório**. No formulário apresentado clique no botão Enviar para verificar os IPs de origem/destino e as portas que estão gerando tráfego.
7. Na janela de relatório, marque a caixa **Traduzir fluxos para a aplicação** para verificar as aplicações para cada linha.

Capítulo 4. Gerador de gráfico Telcomanager

O menu Dados históricos será utilizado para visualizar todos os gráficos do sistema. Abaixo deste menu estão os objetos monitorados do sistema, como dispositivos e interfaces. Quando você clica em um ícone de objeto, seus gráficos serão mostrados na área de seleção de gráficos. Quando você clica em um ícone nesta área, o Telcographer é carregado na área de display de dados.

O Telcographer é um gerador de gráfico altamente interativo escrito em HTML5. As funções desta aplicação serão explicadas abaixo.

Período

O gráfico lê informações do Banco de Dados da Telco, onde todas as informações são gravadas em uma resolução de 5 minutos.

A informação da resolução de 5 minutos está disponível para todo o período de gravação para cada objeto monitorado.

Gráfico diário

Neste período, a informação é apresentada com o maior nível de detalhes. O período de tempo é de 24 horas. Possui uma amostra para cada 5 minutos e 288 amostras no total.

Gráfico semanal

Cada amostra é um valor médio de 6 amostras de 5 minutos, que corresponde a 30 minutos. O período de tempo é de 7 dias com 336 amostras. A curva de máximo é obtida calculando o valor máximo para cada 6 amostras de 5 minutos.

Gráfico mensal

Cada amostra é um valor médio de 24 amostras de 5 minutos, que corresponde a 2 horas. O período de tempo é de 30 dias com 360 amostras. A curva de máximo é obtida calculando o valor máximo para cada 24 amostras 5 minutos.

Gráfico trimestral

Cada amostra é um valor médio de 72 amostras de 5 minutos, que corresponde a 6 horas. O período de tempo é de 90 dias com 360 amostras. A curva de máximo é obtida calculando o valor máximo para cada 72 amostras de 5 minutos.

Gráfico anual

Cada amostra é um valor médio de 288 amostras de 5 minutos, que corresponde a um dia. O período de tempo é de 364 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 288 amostras de 5 minutos.

Gráfico bienal

Cada amostra é um valor médio de 576 amostras de 5 minutos, que correspondem a dois dias. O período de tempo é de 728 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 576 amostras de 5 minutos.

Gráfico de cinco anos

Cada amostra é um valor médio de 1440 amostras de 5 minutos, que correspondem a 5 dias. O período de tempo é 1820 dias com 364 amostras. A curva de máximo é obtida calculando o valor máximo para cada 1440 amostras de 5 minutos.

Gráfico customizado

Você pode escolher um período customizado para o seu gráfico. Para isso, selecione o período **Personalizado** e defina as datas e horários de início de fim.

Recursos

O Telcographer possui diversos recursos que podem ser acessados através do painel de controle acima do gráfico. Alguns deles podem ser acessados também clicando com o botão direito do mouse em qualquer ponto do gráfico.

Caixa de estatísticas

Ao movimentar o mouse sobre uma curva na legenda do gráfico, será mostrada uma caixa de estatísticas com as seguintes informações: Mínimo, Máximo, Média, Total e Desvio padrão da curva.

Mostrar valor

Este recurso irá fazer com que o ponteiro do mouse mostre os eixos x e y para a posição do ponteiro.

Zoom vertical

Para usar este recurso, siga os passos abaixo:

1. Selecione a opção no menu Opções do painel de controle do gráfico.
2. Pressione e segure o botão do mouse na posição inicial y desejada.
3. Enquanto estiver segurando o botão, mova o cursor do mouse para a posição final y desejada e solte o botão do mouse.

Uma curva

Clique nesta opção no menu Opções do painel de controle do gráfico e depois clique em uma das curvas na legenda. Esta ação irá fazer com que seja mostrado no gráfico apenas a curva selecionada.

Modo relativo

Clique nesta opção no menu Opções do painel de controle do gráfico para mostrar cada curva no gráfico relacionada com as outras curvas. Isso significa que, para cada amostra, o somatório dos dados representa 100%.

Este modo funciona apenas se todas as curvas do gráfico estiverem empilhadas.

Configuração de eixos

Clique nesta opção no menu Opções do painel de controle do gráfico para abrir a janela na qual será possível selecionar as curvas que irão aparecer utilizando a escala direita ou esquerda do eixo x.

Associar a Graph Set

Clique com o botão direito do mouse e depois nesta opção para abrir uma caixa onde você será capaz de associar o gráfico a um graphset criado anteriormente.

Salvar imagem

O ícone **Salvar imagem** no painel de controle do gráfico irá salvar o gráfico como uma imagem jpeg.

Tipo de gráfico

Através do menu **Tipo de gráfico** no painel de controle, você pode escolher o tipo de visualização do gráfico: em linha, pizza ou barra.

Gráfico agregado

Clique nesta opção através do menu popup do gráfico para abrir representações agregadas do gráfico. Existem duas opções de gráficos: pizza e barra. Estes gráficos podem ser filtrados por um período do dia. Por exemplo, se você abrir um gráfico em pizza de um gráfico semanal e filtrar das 10:00h às 17:00h, o gráfico em pizza irá representar os dados semanais para aquele período do dia.

Mesmo se você não habilitar o filtro, você pode configurar o período do gráfico usando o campo **Horário útil**. Quando este campo está configurado com **1 dia**, aparece um outro campo: **Últimas horas**, que refere-se às horas que serão consideradas no gráfico. Por exemplo, quando este campo está configurado com o valor 1, isso significa que o gráfico está considerando apenas a última hora. O valor máximo que pode ser configurado é o **24**, que representa as últimas 24 horas.

Dica

Para retirar alguma curva do gráfico, basta clicar nela na legenda.

Aproximar e afastar

Utilize essas funções no menu do popup do gráfico para dar zoom in ou zoom out, respectivamente, na escala do tempo. Por exemplo, utilizando isto em um gráfico anual, é possível dar um zoom in no gráfico diário em um dia particular.

Importante

Essas opções apenas são disponíveis em gráficos do tipo linha.

Exportar

Clique no gráfico com o botão direito do mouse e acesse esta opção. Os dados do gráfico podem ser exportados nos formatos HTML, CSV ou TSV.

Atualização automática

Selecione esta opção para o gráfico ser atualizado automaticamente a cada 5 minutos. Esta opção deve ser previamente habilitada em **Sistema** → **Parâmetros** → **Grafador**, onde você também pode configurar o intervalo de atualização.

Relatório

A partir de qualquer gráfico, é possível gerar um relatório que irá buscar os fluxos utilizados na construção do gráfico.

Clique com o botão direito em qualquer ponto na área do gráfico e mova o mouse até a opção **Relatório de dados brutos**. Depois disso, você pode gerar um relatório customizado ou um pré-configurado.

Isso também é possível através do menu **Relatório de dados brutos** no painel de controle.

Alarmes pré-configurados disponíveis:

- Top IPs de origem
- Top IPs de destino
- Top AS de origem
- Top AS de destino
- Top conversas
- Tráfego não mapeado

Dica

Os gráficos em **Pacotes/s** (pps) e **Bit/s** (bps) possuem uma curva para configuração de sample não aplicada. Logo, para verificar a informação desta curva, passe o mouse sobre a legenda com o nome "No sample total".

Teclas

Algumas teclas do seu teclado possuem funcionalidades especiais. Veja abaixo quais são elas e suas descrições.

Tabela 4.1. Teclas

| Tecla | Descrição |
|-------|---|
| D | Transforma o gráfico para o modo derivativo. |
| I | Indica informações detalhadas sobre o gráfico como resolução, curvas, samples e timestamps. |
| L | Relaciona o timestamp e o valor de cada ponto de uma curva. |
| N | Muda o formato das curvas do gráfico, uma vez que todas elas estejam empilhadas. |
| P | Gera uma curva de projeção que considera apenas os pontos entre o intervalo limitado pelas linhas |

| Tecla | Descrição |
|-------|---|
| | sinalizadas. Quando você move o mouse para baixo, o número de pontos diminui, caso contrário, o número de pontos aumenta. |
| R | Ajusta o gráfico de forma que ele tenha a resolução máxima. |
| S | Salva o gráfico como uma imagem no formato PNG. |
| W | Muda a configuração da curva para waas accell. |
| - | Zoom out. |
| + | Zoom in. |
| LEFT | Desloca o gráfico para esquerda. |
| RIGHT | Desloca o gráfico para direita. |
| * | Gráfico retorna ao seu tamanho normal. |

Dica

Você pode converter o tempo em timestamp para data usando o comando **ts2date** na CLI.

Capítulo 5. Dados históricos

Este capítulo descreve os elementos da guia de dados históricos.

Abaixo desta guia você pode acessar todos os dados processados pelos objetos monitorados.

Os dados podem ser acessados através de gráficos e relatórios.

Resumo da rede

Esta aba disponibiliza um resumo do tráfego absoluto na sua rede na última hora.

Os dados podem ser visualizados em forma de lista, gráfico em pizza ou gráfico em barra.

Você pode configurar quais tipos de objetos serão exibidos nesse resumo bem como que tipo de visualização cada um terá.

Importante


Se você arrastar os Top 10 de forma que altere a ordem de exibição e/ou remover algum deles usando o "X", o sistema irá salvar essas alterações.

Os tipos de objetos disponibilizados nesse resumo são:

- Aplicação
- Dispositivo
- Grupo de aplicações
- Grupo de interfaces
- Grupo de sistemas autônomos
- Grupo de subredes
- Grupo de ToS
- Objeto mapeado
- Protocolo
- Sistemas autônomos
- Subrede
- ToS

Dica

Clique com o mouse sobre um objeto para abrir o gráfico dele em uma nova aba.

Para abrir esta aba em uma nova janela, use o ícone .





Para configurar os objetos exibidos e seus tipos de visualização, clique no ícone . Depois disso, selecione e arraste os elementos para configurar a ordem de exibição. Veja abaixo o significado de cada ícone.

Tabela 5.1. Tabela de ícones

| Ícone | Descrição |
|---|---|
|  | Mostra o top 10 dos objetos em forma de lista. |
|  | Mostra o top 10 dos objetos em forma de gráfico em pizza. |
|  | Mostra o top 10 dos objetos em forma de gráfico em barra. |

Favoritos

Usando este recurso, cada usuário pode configurar os objetos de interesse para acesso rápido.

Adicionando objetos aos favoritos

Para adicionar objetos aos seus favoritos, simplesmente clique no ícone da estrela dourada mostrado como primeiro elemento da área do gráfico selecionada para o objeto desejado.

Removendo objetos dos favoritos

Para remover objetos dos seus favoritos, simplesmente clique no ícone da estrela dourada como primeiro elemento da área do gráfico selecionada para o objeto desejado.

Totais

Esta guia contém apenas 3 gráficos, que representam o tráfego para um domínio.

Subredes

Os objetos de subredes permitem a análise de blocos IP. Também é possível usar o objeto do grupo de subrede para criar um conjunto de subredes para ser analisada.

Definições

- **Tráfego de destino da subrede:** composto pelo somatório de todos os fluxos em que o endereço de IP de destino pertence ao bloco de IP de subrede.
- **Tráfego de origem da subrede:** composto pelo somatório de todos os fluxos em que o endereço de IP de origem pertence ao bloco de IP da subrede.

Configuração

Para gerenciar o sistema de subredes, acesse **Dados Históricos** → **Subredes**.

Clique no item de menu da árvore **Subredes** para ter a lista de subredes configuradas.

Para adicionar uma nova subrede, clique no botão **Novo** e preencha o formulário.

Tabela 5.2. Formulário de nova subrede

| Campos | Descrição |
|--|--|
| Nome | Nome da subrede. |
| Descrição | Descrição de subrede. |
| Blocos de endereço IP | Subredes podem ter mais que uma faixa de endereços. Ex: 10.0.0.0/24, 10.0.1.0/24, 2001:db8:abcd:2000::/64, 2001:cdba:9abc:5678::/64. |
| Tráfego limite (bps) | Este valor será plotado no gráfico do objeto como uma linha pontilhada vermelha. |
| Threshold do Fator de Atividade de origem | Limite do Fator de Atividade de origem. |
| Threshold do Fator de Atividade de destino | Limite do Fator de Atividade de destino. |
| Habilitar projeção | Use os parâmetros padrão de projeção ou defina-os. Vá à seção de Projeção para dicas de como configurar estes parâmetros. |
| Perfil de ameaça | Selecione um perfil de ameaça para esta subrede para ser usado na Análise de ameaças ou deixe em branco. |
| Grupo de subredes | Associação de grupo de subredes. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Selecione o perfil de tráfego de uma maneira que ele possa ser aplicado a esta subrede. |
| Perfil de alarme | Associação de perfil de alarme. |

Importar arquivos de subredes

Para importar um arquivo de subrede, acesse **Dados históricos** → **Subredes**.

Clique no item **Subredes** no menu da árvore.

Clique no botão de importar e carregar o arquivo.

Uma subrede importada possui os seguintes campos:

Tabela 5.3. Campos de um arquivo de subrede

| Campo | Descrição |
|------------------------------|---|
| Nome | Possíveis caracteres para campo de nome. |
| Descrição | Caracteres gerais (opcional). |
| Blocos de endereço IP | Subredes podem ter mais que uma faixa de endereços. Formato de entrada: IP1/Máscara1,IP2/Máscara2. (IP/32 no caso de usar um IP único). Ex: 10.0.0.1/32,10.0.1.0/24 |
| Tráfego limite (bps) | Valores inteiros maiores ou iguais a 0. |
| Habilitar análise de ameaças | Preencha com yes ou no . |

Grupo de subredes

Grupos de subredes podem ser utilizados para organizar suas subredes.

Definições

- O tráfego do grupo é um somatório de cada bloco IP individual da subrede contida no grupo. Isto significa que blocos IPs duplicados serão somados apenas uma única vez no tráfego de grupo.
- Quando um grupo de subrede é criado, ele deve ser associado a um grupo de nível superior, o que é apenas organizacional.
- O TRAFip tem como padrão três desses grupos e o usuário pode modificar o nome deles e criar mais em **Dados históricos** → **Subredes** → **Lista de agrupamento** .

Configuração

Para gerenciar o grupo de subredes acesse, **Dados históricos** → **Subredes**.

Clique no item **Grupo de subredes** no menu da árvore para ter a lista de subredes configuradas.

Para adicionar uma nova subrede, preencha o formulário abaixo de acordo com o estipulado:

Tabela 5.4. Formulário de grupo de subredes

| Campo | Descrição |
|----------------------------|---|
| Nome | Nome do grupo de subrede. |
| Descrição | Descrição da subrede. |
| Habilitar projeção | Parâmetros padrão para projeção. Vá à seção de Projeção para dicas de como configurar estes parâmetros. |
| Tráfego limite (bps) | Este valor será plotado no objeto gráfico como uma linha pontilhada vermelha. |
| Agrupamento | Nível organizacional mais alto. |
| Subredes | Subrede pertencente a este grupo. |
| Perfil de alarme | Associação de perfil de alarme. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Selecione o perfil de tráfego de uma maneira que ele possa ser aplicado a esta subrede. |

Agrupamento

Este objeto é apenas a nível organizacional onde você pode usar para organizar os grupos de subredes do TRAFip.

Cada grupo de subrede pode ser posicionado em apenas um único agrupamento.

Para gerenciar o agrupamento acesse no menu, **Dados históricos** → **Subredes** → **Lista de Agrupamentos**

Para adicionar um novo agrupamento, preencha o formulário de acordo com o descrito abaixo:

Tabela 5.5. Novo formulário de agrupamento

| Campo | Descrição |
|-----------------------|----------------------------------|
| Nome | Nome do agrupamento |
| Grupos de agrupamento | Associação de grupos de subredes |

Dispositivos

Para mapear física e logicamente os dispositivos como interfaces, o sistema possui um processo de mapeamento que roda periodicamente e mapeia (Veja a seção: Configuração de mapeadores). Existe um mapeador pré-configurado para mapear interfaces de dispositivos que usam ifDescr OID para executar esta tarefa.

Procedimento 5.1. Passos da configuração dos dispositivos

1. Selecione **Dados históricos** → **Dispositivos** → **Dispositivo** .
2. Clique no botão **Novo** e preencha o formulário abaixo.

Tabela 5.6. Formulário de novo dispositivo

| Campo | Descrição |
|-------------------------|---|
| Nome | Nome do dispositivo. |
| Descrição | Descrição do dispositivo. |
| Endereço IP de gerência | Endereço de IP do dispositivo. Este endereço de IP deve responder às consultas SNMP para o monitoramento SNMP e às requisições ICMP echo para monitoramento ICMP. |
| Tipo | Tipo do dispositivo, o usuário pode usar este campo para categorizar livremente todos os dispositivos configurados. |
| Fabricante | Nome do fabricante do dispositivo. |
| Latitude | Coordenada geográfica, no formato de graus decimais (DD, na sigla em inglês), usada para que o dispositivo seja localizado em mapas georreferenciados. Exemplo: -22.9035. |
| Longitude | Coordenada geográfica, no formato de graus decimais (DD, na sigla em inglês), usada para que o dispositivo seja localizado em mapas georreferenciados. Exemplo: -43.2096. |
| Credencial de SNMP | Escolha uma credencial de SNMP. |
| Versão do SNMP | Selecione a versão SNMP. Os possíveis valores são: SNMP v1 ou SNMP v2c Especifica uma community SNMP |

| Campo | Descrição |
|---------------------------------------|---|
| | SNMP v3 Especifica o tipo de autenticação e seus parâmetros |
| Community SNMP | Preencha a community SNMP. |
| Utilizar configuração padrão de SNMP | Esta opção deixa você definir valores que podem ser usados especificamente para este dispositivo. Os valores padrões são especificados na configuração dos parâmetros dos coletores SNMP. |
| Considerar SysUpTime na coleta | Descarta a coleta se o dispositivo não é permitido por mais de 5 minutos. Previne erros de cálculo. |
| SNMP Timeout | Tempo limite em segundos para esperar por uma resposta de pacote SNMP. Intervalo de valores: 1-10. |
| Tentativas SNMP | Número de novas tentativas que serão permitidas para o dispositivo se ele não responder a uma consulta SNMP. Intervalo de valores: 1-10. |
| Número de OIDs por pacote | Número de OIDs que serão enviadas em cada pacotes SNMP. Intervalo de valores: 1-100. |
| Taxa máxima de envio de pacotes (pps) | Número máximo de pacotes por segundo que uma coletora SNMP irá enviar para cada dispositivo. |
| Janela SNMP | Número de pacotes SNMP que serão enviados sem resposta do dispositivo que está sendo polled. |
| Porta SNMP | A porta SNMP. |
| Agentes | Esta opção permite que você defina múltiplos agentes SNMP no mesmo endereço de IP e diferentes portas. Agora você pode especificar máscaras OID e a porta SNMP para esta máscara. Isto significa que o coletor SNMP usará a porta UDP especificada se a OID a ser coletada neste dispositivo corresponder à máscara especificada. Exemplo: <ul style="list-style-type: none"> • Prefixo OID .1.3.4.6.9.9.1.2.* Porta SNMP: 163 • Prefixo OID .1.3.4.6.9.9.1.3.* Porta SNMP: 164 |
| Credencial de conexão | Escolha uma credencial de conexão. |
| Protocolo de conexão | Escolha entre SSH ou Telnet . |
| Porta SSH | Quando o Protocolo de conexão é SSH, entre com a porta SSH. O valor padrão é 22 . |

| Campo | Descrição |
|------------------------------------|--|
| Porta Telnet | Quando o Protocolo de conexão é Telnet, entre com a porta Telnet. O valor padrão é 23 . |
| Usuário | Usuário para ser usado para acessar o dispositivo. Esta string está disponível como um campo livre %username% para scripts de provisionamento. |
| Senha do usuário | Senha a ser usada para acessar o dispositivo. Esta string está disponível como um campo livre %passwd% para scripts de provisionamento. |
| Senha de enable | Senha de enable é usada para acessar o dispositivo. Esta string está disponível como um campo livre %enable_passwd% para scripts de provisionamento. |
| Habilitar coleta pelo TRAFip | Habilita a coleta pelo TRAFip. |
| Endereços IP do Netflow exporter | Preencha o endereço de IP que o netflow exporter irá usar para enviar fluxos. Ao lado deste campo, tem um ícone de lupa. Clique nele para preencher automaticamente usando como base o Endereço de IP do dispositivo. |
| Configuração de sampling rate | Pode ser setada manualmente ou baseada em um fluxo. |
| Netflow sampling rate | Se você está exportando fluxos, escolha se considerará uma taxa manual configurada ou se detectará a taxa dos registros de fluxos. |
| Habilitar coleta pelo SLAview | Habilita a coleta pelo SLAview. |
| Perfis automáticos | Selecione esta opção para habilitar o uso desse dispositivo e seus objetos mapeados em perfis automáticos. A associação só irá ocorrer se o dispositivo ou seus objetos corresponderem às regras de perfil. (Veja a seção de configuração de perfil) . |
| Habilitar gerência de configuração | Habilita a gerência de configuração pelo CFGtool. |
| Modo de exportação de configuração | Selecione Ativo para exportar a configuração periodicamente de acordo com o tempo configurado em Sistema → Parâmetros → Gerência de configuração . Para exportar a configuração usando filtro de trap, selecione Passivo . |
| Método de mapeamento de topologia | Selecione o protocolo que será usado para o mapeamento de topologia. As opções disponíveis são: CDP - Cisco Discovery Protocol, LLDP - Link Layer Discovery Protocol ou ambos. Usando ambos os métodos, o SLAview utilizará o protocolo SNMP para buscar informações destes protocolos nas tabelas MIB dos dispositivos monitorados. |

| Campo | Descrição |
|--------------------------------------|--|
| Habilitar provisionamento | Habilitar provisionamento para configurar automaticamente as Cisco IP SLA probes, Telcomanager probes e exportação de Netflow. |
| Coletor | Associação do dispositivo a um coletor remoto. Este campo está disponível apenas quando a arquitetura distribuída é habilitada. |
| Script de autenticação | Quando o protocolo de conexão estiver configurado como Telnet , você precisa selecionar um script de Login. |
| Script para provisionamento | Preencha esta opção para provisionamento de Netflow em sistemas com arquitetura distribuída e configuração de probes. Este script será usado para reconfigurar exportação de Netflow para um coletor de backup se o coletor falhar. |
| Templates de polling | Escolha um template do polling ICMP para o dispositivo. O template de polling permite que você configure os tempos específicos para capturar os dispositivos e medir a disponibilidade deles. |
| Tipo de dispositivo | Campo usado para escolher um ícone para representar o dispositivo graficamente nos Mapas. É possível escolher entre: Câmera, Firewall, Roteador, Servidor, Switch ou Sem Fio. O tipo padrão é o Roteador . |
| Script de exportação de configuração | Selecione os scripts exportadores de configuração dos tipos running e startup. |
| Domínio | Associação de domínio do dispositivo. |
| Grupos | Clique no botão de Listar e selecione os grupos desejados para este dispositivo em um ou mais pontos no grupo de hierarquia. |
| Mapeadores | Selecione o mapeador desejado para mapear objetos, como interfaces e cpus neste dispositivo.(Veja a seção configuração de mapeadores.) |
| Perfis de alarme | Associa o dispositivo a um perfil de alarme. |

Criando um dispositivo utilizando o Assistente

Existe um assistente para criação de um dispositivo que irá guiá-lo e validará cada passo.

1. Selecione **Dados Históricos** → **Dispositivos** → **Assistente** .
2. Preencha os campos de acordo com a tabela acima.
3. Durante a criação, você é capaz de testar a conectividade do equipamento, mapear os objetos do dispositivo e testar os objetos associados aos perfis, por exemplo.

4. Depois disso, você pode visualizar e salvar seu novo dispositivo.

Verificando objetos mapeados para o dispositivo

Clique no ícone de objetos mapeados no menu lateral em árvore para ver todos os objetos mapeados do sistema. Acessando o formulário de cada um, você pode habilitar projeção e adicionar uma descrição para o objeto.

Também é possível checar o histórico de configuração e deletar o objeto usando, respectivamente, os botões **Histórico** e **Apagar**.

Existe um filtro no topo da página com opções para selecionar objetos localizados e não localizados. Objetos não localizados são objetos mapeados que não foram localizados por um mapeador do dispositivo. Ex: um módulo de interface que foi removido por um roteador irá levar esta interface a um estado de não localizado.

Na área do menu em árvore, abaixo de cada dispositivo, o sistema mostra os seus respectivos objetos mapeados. A cor dos ícones indica as seguintes condições:

| | |
|-------------------------|---|
| Ícone verde | O objeto tem um perfil associado a ele. |
| Ícone sem cor | O objeto não tem um perfil associado a ele. |
| Ícone vermelho piscando | O objeto não foi localizado pelo mapeador de processos do objeto. |

Importar arquivos de dispositivo

Para importar um arquivo de dispositivo, acesse **Dados históricos** → **Dispositivos**.

Clique no item **Dispositivos** na árvore de menu.

Clique no botão **Importar** e carregue o arquivo.

Um arquivo de dispositivos importados tem os seguintes campos:

Tabela 5.7. Campos do arquivo de dispositivo

| Campo | Descrição |
|-------------------------|--|
| Nome | Possíveis caracteres para o campo de nome. |
| Descrição | Possíveis caracteres para o campo de descrição (opcional). |
| Endereço IP de gerência | Endereço de IP. Ex.: 10.0.0.1 |
| Versão SNMP | Tipo 1 para versão 1, 2c para versão 2 e 3 para versão 3. |
| Community SNMP | Possíveis caracteres para Community SNMP. |
| Protocolo de conexão | Escreva SSH ou TELNET . |
| Usuário | Possíveis caracteres para campo de nome (opcional). |

| Campo | Descrição |
|----------------------------------|--|
| Senha de usuário | Possíveis caracteres para campo de senha (opcional). |
| Senha de enable | Possíveis caracteres para campo de senha (opcional). |
| Habilitar coleta pelo TRAFip | SIM para habilitar e NÃO para desabilitar a coleta pelo TRAFip. |
| Endereço IP do Netflow exporters | Lista de endereço IP separada por vírgula. Ex.: 10.0.0.1,10.0.0.2 |
| Configuração de sampling rate | Terá o valor 0 para manual e o valor 1 para fluxo. |
| Netflow sampling rate | Valor inteiro maior que 0. |
| Habilitar coleta pelo SLAview | SIM para habilitar e NÃO para desabilitar a coleta pelo SLAview. |
| Perfil automático | Selecione SIM para habilitar o uso deste dispositivo e seus objetos em um perfil automático. |
| Tipo de dispositivo | Campo usado para escolher um ícone para representar graficamente o dispositivo nos mapas. Escolha Câmera, Firewall, Roteador, Servidor, Switch ou Sem Fio. |

Importante

Se o ícone do dispositivo ficar vermelho, significa que todos os exportadores estão indisponíveis.

Grupos de interface

Grupos de interfaces permitem análises detalhadas de uma única interface ou de um grupo de interface, porque perfis podem ser aplicados a eles e uma interface pode ser associada a mais de um grupo de interface.

Para criar um novo grupo de interface, acesse no menu **Dados históricos** → **Dispositivos** → **Grupo de interface** e clique no botão **Novo**.

Tabela 5.8. Formulário de grupos de interface

| Campo | Descrição |
|--------------------------------------|---|
| Nome | Nome do grupo de interface. |
| Descrição | Breve descrição do grupo de interface. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| Habilitar projeção | Parâmetros padrão da projeção. Para dicas de como configurar estes parâmetros, vá à seção Projeção. |
| Agrupamento para grupo de interfaces | Grupo de interface de nível mais alto, apenas organizacional. Acesse Configuração → Objetos → Agrupamento para grupo de interfaces para configurar novos grupos. |
| Domínio | Domínio a qual grupo esta interface pertence. |

| Campo | Descrição |
|----------------------------|---|
| Interfaces | Selecione a interface que pertence a este grupo. |
| Perfil de alarme | Associação a um perfil de alarme. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Selecione o Perfil e como ele deve ser aplicado a esta interface. |

Tráfego não mapeado

É assim chamado todo tráfego que não possui uma interface de entrada ou uma interface de saída. Isto pode ocorrer por diversas razões: perda de pacote, tráfego destinado ou originado para o próprio dispositivo, problema de roteamento, etc.

Aplicações

O objeto de aplicação é representado por uma regra que combina endereços de IP, portas e um protocolo da camada 4 do modelo OSI.

Acesse **Dados históricos** → **Aplicações** → **Aplicação** para gerenciar as aplicações correntes configuradas e adicionar novas.

Tabela 5.9. Formulário de aplicação

| Campo | Descrição |
|-----------------------------------|---|
| Nome | Nome da aplicação. |
| Descrição | Breve descrição da aplicação. |
| Tráfego limite (bps) | Este valor será plotado no gráfico como uma linha vermelha pontilhada. |
| Identificação por ID de aplicação | Habilite este campo para identificar a aplicação pela sua ID. |
| Subrede(s) de origem | Subredes para combinar contra o campo de fluxo de endereço de IP de origem. Ex: 10.0.0.0/24,10.1.0.0/16,192.168.1.1/32. |
| Portas de origem | Portas para combinar contra o campo de fluxo da porta de origem. |
| Operação | Operação para ser realizada entre os campos de origem e destino. Ex: 80,443-446,455 |
| Subrede(s) de destino | Subredes para combinar contra o campo de fluxo de endereço de IP de destino. |
| Porta de destino | Portas para combinar contra o campo de fluxo da porta de destino. |
| Classification engine ID | Um registro específico para as atribuições da aplicação. |
| Selector ID | Um registro específico para as atribuições da aplicação. |
| Grupo de aplicação | Faça a associação da aplicação com os grupos de aplicação, se desejar. |

| Campo | Descrição |
|-------------------|--|
| Protocolos | Selecione a camada 4 do protocolo OSI para usar nesta aplicação. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |

Classificação

As aplicações serão classificadas de acordo com a prioridade listada em **Dados históricos** → **Aplicações** → **Aplicação** .

Cada fluxo irá corresponder a uma única aplicação.

Para mudar a prioridade de classificação, selecione uma ou mais aplicações e clique nas setas para CIMA ou para BAIXO que aparecem do lado esquerdo acima da lista de aplicação.

Importar arquivos de aplicação

Para importar um arquivo de aplicação, acesse **Dados históricos** → **Aplicações**.

Clique no item **Aplicações** na árvore de menu.

Clique no botão **Importar** e carregue o arquivo.

Uma importação de aplicação tem os seguintes campos:

Tabela 5.10. Campos de arquivo de aplicação

| Campo | Descrição |
|-----------------------|--|
| Nome | Possíveis caracteres para o campo Nome. |
| Descrição | Caracteres gerais (opcional). |
| Tráfego limite (bps) | Valor inteiro maior ou igual a 0. |
| Subrede(s) de origem | Lista de subrede. Formato de entrada: IP1/Máscara1,IP2/Máscara2. (IP/32 no caso de usar um IP único). Ex: 10.0.0.0/24,10.0.1.0/24. Você pode usar * para todas as subredes de origem. |
| Portas de origem | Lista de inteiros entre 1 e 65535, separados por vírgula. Você pode usar * para todas as portas de origem. |
| Operação | Entre 1 para operação OU , 2 para operação E. |
| Subrede(s) de destino | Lista de subrede. Formato de entrada: IP1/Máscara1,IP2/Máscara2. (IP/32 em caso de usar um IP único). Ex: 10.0.0.0/24,10.0.1.0/24. Você pode usar * para todas as subredes de destino. |
| Porta de destino | Lista de inteiro entre 1 e 65535, separados por vírgula. Você pode usar * para todas as portas de destino. |
| Protocolos | Camada 4 do protocolo OSI, separado por vírgula. Ex: UDP,TCP (opcional). |

Grupos de aplicação

Grupos de aplicação serão úteis para organizar suas aplicações. Usando esse tipo de objeto, você poderá ter uma visão consolidada de um grupo de aplicações.

Para configurar um novo grupo de aplicação, acesse o menu **Dados Históricos** → **Aplicações** → **Grupo de aplicação**.

Tabela 5.11. Formulário de grupo de aplicações

| Campo | Descrição |
|----------------------|--|
| Nome | Defina um nome. |
| Descrição | Descreva o novo grupo de aplicação. |
| Tráfego limite (bps) | Este valor será plotado no gráfico como uma linha vermelha pontilhada. |
| Aplicação | Selecione as aplicações a serem associadas a esse grupo de aplicação. |
| Perfil de tráfego | Acesse a seção Perfil de tráfego. |

Protocolos

Este objeto se refere a camada de transporte do modelo TCP/IP. Ele é representado, basicamente, por um número indicando o protocolo de cada fluxo. Exemplo: 17 para tráfego UDP e 6 para tráfego TCP.

Acesse **Dados históricos** → **Protocolos** → **Protocolo** para gerenciar os protocolos configurados e adicionar novos.

Tabela 5.12. Formulário de protocolo

| Campo | Descrição |
|----------------------|---|
| Nome | Nome do protocolo. |
| Descrição | Descrição do protocolo. |
| Número | Número do protocolo. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |

Importar arquivos de protocolos

Para importar um arquivo de protocolos, acesse **Dados históricos** → **Protocolos**.

Clique em **Protocolos** na árvore do menu.

Clique no botão **Importar** e carregue o arquivo.

Um protocolo importado possui os seguintes campos:

Tabela 5.13. Campos do arquivo de protocolo

| Campo | Descrição |
|----------------------|---|
| Nome | Possíveis caracteres para o campo Nome. |
| Número | Valor inteiro entre 0 e 255. |
| Descrição | Caracteres gerais (opcional). |
| Tráfego limite (bps) | Valor inteiro maior ou igual a 0. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |

Sistemas autônomos

Como definido no RFC 1930, um sistema autônomo é uma coleção de prefixos de roteamento IP conectados sobre controle de um ou mais operadores de redes que representa uma comum, claramente definida, política de roteamento para internet.

Este objeto combina o campo de AS origem do fluxo para formar seu tráfego de origem e o campo de AS destino do fluxo para formar seu tráfego de destino.

Dica

Alguns roteadores podem preencher o campo de AS do fluxo com o AS destino final/origem ou com as informações de pareamento do AS. Nos roteadores Cisco, você pode configurar o comando:

```
ip flow-export version {1|5|9 [origin-AS|peer-AS/]}
```

Para configurar um novo AS, acesse **Dados históricos** → **Sistemas autônomos** → **Sistema autônomo** .

Tabela 5.14. Formulário de sistemas autônomos

| Campo | Descrição |
|----------------------------|---|
| Nome | Nome AS. |
| Descrição | Descrição AS. |
| Habilitar projeção | Parâmetros padrões da projeção. Acesse a seção Projeção para dicas de como configurar estes parâmetros. |
| Número | Número AS. Para configurar uma lista de números, separe-os por vírgula. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| Grupo de AS | Associação de grupo AS. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Selecione o perfil e como eles devem ser aplicados a este AS. |

Importar arquivos de sistemas autônomos

Para importar um arquivo do dispositivo, acesse **Dados históricos** → **Sistemas autônomos**.

Clique no item **Sistema autônomo** na árvore do menu.

Clique no botão **Importar** e carregue o arquivo.

Um sistema autônomo importado possui os seguintes campos:

Tabela 5.15. Campos de um arquivo de sistema autônomo

| Campo | Descrição |
|----------------------|---|
| Nome | Possíveis caracteres para o campo de nome. |
| Número | Lista de inteiros entre 1 e 65535, separados por vírgula. |
| Descrição | Caracteres gerais (opcional). |
| Tráfego limite (bps) | Valor inteiro maior ou igual a 0. |

Grupo de sistema autônomo

Você pode usar grupos AS para ter uma visão consolidada de um grupo de sistemas autônomos. Por exemplo, os ASs de cada continente.

Para configurar um novo grupo de AS, acesse **Dados históricos** → **Sistema autônomo** → **Grupo de sistema autônomo**.

Tabela 5.16. Formulário de grupo de sistemas autônomos

| Campo | Descrição |
|----------------------------|--|
| Nome | Nome de AS. |
| Descrição | Descrição de AS. |
| Habilitar projeção | Parâmetros padrões da projeção. Acesse a seção de projeção para dicas de como configurar estes parâmetros. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| Sistema autônomo | Sistemas autônomos que devem ser colocados neste grupo. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Seleciona o perfil e como eles devem ser aplicados neste grupo de AS. |

Tipo de serviço

O objeto de tipo de serviço representa o campo ToS do cabeçalho do endereço IP. Este campo é exportado para cada fluxo e não tem origem nem destino.

Este campo é usualmente utilizado para marcar pacotes que estão na borda da rede, logo eles podem ser tratados com a política QoS apropriada pelos roteadores principais.

Importante

Esteja ciente que o netflow Cisco não vai exportar o campo ToS com o valor correto do tráfego saindo pela borda dos roteadores para os roteadores da rede principal se os pacotes forem marcados na interface WAN. Logo, apenas pacotes vindos dos roteadores principais irão possuir valores exportados corretos no campo de ToS, porque eles já estão marcados quando

chegam a borda do roteador. Para ter o fluxo de pacotes vindos do roteador principal marcados corretamente, você deve marcar os pacotes na interface LAN.

Para gerenciar os objetos ToS, acesse **Dados históricos** → **ToS** → **ToS** .

Tabela 5.17. Formulário de ToS

| Campo | Descrição |
|----------------------------|--|
| Nome | Nome ToS. |
| Descrição | Descrição do ToS. |
| Número | Número do ToS. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| Habilitar projeção | Parâmetros padrões da projeção. Acesse a seção de projeção para dicas de como configurar estes parâmetros. |
| Grupo ToS | Associação de grupo ToS. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Seleciona o perfil e como eles devem ser aplicados neste grupo de ToS. |

Importar arquivos ToS

Para importar um arquivo ToS, acesse **Dados históricos** → **ToS**.

Clique no item **ToS** na árvore do menu.

Clique no botão Importar e carregue o arquivo.

Um arquivo ToS importado possui os seguintes campos:

Tabela 5.18. Campos dos arquivos ToS

| Campo | Descrição |
|----------------------|--|
| Nome | Possíveis caracteres para campo de nome. |
| Número | Inteiro entre 1 e 65535, separado por vírgula. |
| Descrição | Caracteres gerais (opcional). |
| Tráfego limite (bps) | Valor inteiro maior ou igual a 0. |

Grupo de ToS

Você pode usar os grupos ToS para ter uma visão consolidada de um grupo de ToS. Por exemplo, os ToS usados para marcar o tráfego de vídeo.

Para configurar um novo grupo de ToS, acesse **Dados históricos** → **ToS** → **Grupo de ToS** .

Tabela 5.19. Formulário de grupo de ToS

| Campo | Descrição. |
|--------------|-----------------------|
| Nome | Nome do grupo de ToS. |

| Campo | Descrição. |
|----------------------------|--|
| Descrição | Descrição do grupo de ToS. |
| Habilitar projeção | Parâmetros padrões da projeção. Acesse a seção de projeção para dicas de como configurar estes parâmetros. |
| Tráfego limite (bps) | Este valor será plotado no gráfico de tráfego como uma linha vermelha pontilhada. |
| ToS | Objetivos ToS que devem ser colocados neste grupo. |
| Perfil de tráfego | Cheque a seção Perfis de tráfego. |
| Caixa de seleção de perfil | Seleciona o perfil e com ele deve ser aplicado neste grupo de ToS. |

Relatórios

Templates

Para a maioria dos relatórios disponíveis no sistema, você tem a opção de salvá-los como template.

Salvando

1. Abra o relatório desejado e selecione a opção Salvar template.
2. Preencha os campos abaixo:

Tabela 5.20. Forma do template

| Campos | Valores |
|-----------------------------|--|
| Nome | Nome do relatório. |
| Permissão de escrita | Selecione quem pode alterar este relatório. Esta opção de grupos é baseada no grupo de usuários. |
| Permissão de leitura | Selecione quem pode ler este relatório. Esta opção de grupos é baseada nos grupos de usuários. |
| Enviar relatório por e-mail | Enviar por e-mail. |
| Formato do anexo | Escolha o formato desejado: PDF or CSV. |

3. Preencha os outros campos de relatório e clique no botão de Enviar.

Depois de executar os passos acima, o relatório salvo estará disponível em **Lista de template** para cada tipo de relatório.

Agendamento

1. Abra a lista de template para o relatório criado ou crie um novo relatório.
2. Selecione a opção Agendar template.
3. Selecione a opção de agendamento apropriada.

Opções de agendamento

- Uma execução: o início e fim de tempo dos dados serão o início e fim do tempo dos relatórios.
- Diário: os dados terão início à 00:00 h e fim às 23:59 h do dia anterior
- Semanal: os dados terão início no Domingo à 00:00 h e fim no Sábado da semana anterior às 23:59 h.
- Mensal: os dados terão início no dia 01 à 00:00 h e fim no último dia do mês anterior às 23:59 h.

Dica

Para agendar um relatório, você deve salvá-lo como template.

Dica

Quando um relatório está pronto, ele é enviado para o e-mail dos usuários. O servidor SMTP deve ser configurado, bem como o email para cada usuário no formulário de configuração do usuário.

Editando

Após o template estar salvo, um botão de **Editar** aparecerá na lista de template e pode ser usado para mudar os parâmetros do relatório.

Visualizando relatórios

Depois do sistema rodar um template, um novo relatório é gerado.

Todas as instâncias do relatório podem ser acessadas através do botão **Detalhes** para cada template.

Para visualizar uma instância do relatório, siga o procedimento abaixo:

1. Clique no botão **Detalhes** para o template desejado.
2. Escolha o formato de saída desejado, entre HTML, CSV e PDF.
3. Clique no botão **Mostrar** para a instância de relatório desejada.

Gerenciando espaço de disco

O espaço total disponível e atualmente usado pelos templates de relatório é listado abaixo da lista de template.

O sistema tem uma área de armazenamento reservada que é compartilhada por todos os relatórios.

Você pode aumentar ou diminuir este espaço indo em **Sistema** → **Parâmetros** → **Armazenamento de dados** .

Você pode deletar relatórios gerados clicando no botão **Detalhes** na lista de template, para o template desejado.

Tráfego Suspeito

O relatório de tráfego suspeito fornece informações mais detalhadas a respeito das estatísticas mostradas em **Sistema** → **Diagnósticos** → **Estatística de tráfego suspeito** .

Para gerar um novo relatório, acesse **Dados Históricos** → **Relatórios** → **Tráfego Suspeito** .

O formulário já estará preenchido, mas você poderá editá-lo. Então, clique no botão **Enviar**.

Tabela 5.21. Relatório de Tráfego Suspeito

| Campo | Descrição |
|--------------------|--|
| Instante inicial | Preencha com o horário do início do período. |
| Instante final | Preencha com o horário do fim do período. |
| Filtro por subrede | Selecione Nenhum para não filtrar por Subrede ou selecione a desejada. |
| Número de linhas | Estabeleça um limite de linhas para a saída do relatório. |
| Tipo de Ataque | Você pode escolher entre Alto fluxo de dados entre dois IPs e IP Flood . |
| Formato | Você pode escolher Taxa ou Total . |

Dica

Você pode gerar **relatórios de dados brutos** para obter estatísticas detalhadas e consolidadas para cada fluxo. Para isso, basta clicar no ícone que aparece ao lado de cada endereço IP.

Top N

Definições

Relatórios Top N geram estatísticas consolidadas para todos os tipos de objetos.

O relatório de saída mostrará estatísticas de todos os objetos do tipo selecionado, incluindo o percentual utilizado do tráfego limite.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Top N** .
2. Escolha o tipo de objeto desejado ou um template da lista de templates.
3. Preencha o formulário:

Tabela 5.22. Relatório Top N

| Campos | Descrição |
|-----------------------------------|--|
| Gerar relatório Salvar template | Escolha um relatório de uma única execução ou salve o template. |
| Tipo de objeto | Automaticamente preenchido com o tipo de objeto selecionado. |
| Filtro por nome | Use expressões regulares para filtrar. |
| Filtro de ifAlias | Filtra pela OID ifAlias SNMP, em caso de relatórios de interface. |
| * Fabricante | Filtro pelo fabricante do objeto. Você tem que usar expressões regulares para filtrar. |

| Campos | Descrição |
|------------------------|--|
| * Tipo de fabricante | Filtra por tipo de fabricante do objeto. Você tem que usar expressões regulares para filtrar. |
| Instante inicial | Seleção de data para instante inicial. |
| Instante final | Seleção de data para instante final. |
| Excluir fins-de-semana | Excluir períodos de fins-de-semana do relatório de dados. |
| Intervalo | Se todas as opções estiverem marcadas, este campo será ignorado, senão o dado é selecionado com aquele intervalo para cada dia. |
| Sentido | Escolha um sentido para filtrar o tráfego. Caso você selecione Ambos , você poderá Agrupar por objetos , ou seja, o relatório será ordenado pela maior entrada e saída, mostrando a Origem e o Destino de cada objeto em duas linhas consecutivas. |
| Ordenar por | Este campo só aparece quando o sentido for Ambos . Escolha se o relatório será ordenado por entrada, saída, percentual de uso do limite ou pelo máximo de percentual de uso do limite. |
| Unidade | Escolha a unidade para mostrar o tráfego. |
| Formato de saída | Opção disponível apenas para relatórios que não são de template. A partir do momento que o relatório vira um template esta opção é ignorada. |
| Percentil | Use percentil para computar os resultados do relatório. |

* Disponível apenas para relatórios de Dispositivos, Interfaces e Interfaces SNMP.

Dica

Se você selecionar pacotes ou fluxos abaixo do campo de unidade, você será capaz de detectar atividades suspeitas, como uma subrede com um número de pacotes ou fluxos que não é compatível com o seu tráfego.

Perfil de tráfego

Definições

Este relatório é baseado nos dados sumarizados.

Para ter os dados neste relatório, você precisa configurar objetos e associá-los ao perfil de tráfego, que deve conter outros objetos.

Desta forma, você será capaz de obter uma matriz de tráfego de, por exemplo, subredes por subredes, subredes por aplicações, interfaces por subredes e outros.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Perfil de tráfego** → **Novo relatório** .

2. Preencha o formulário:

Tabela 5.23. Relatório de perfil de tráfego

| Campos | Descrição |
|-----------------------------------|---|
| Gerar relatório Salvar template | Escolha relatório de uma única execução ou salve o template. |
| Domínio | Escolha o domínio. |
| Tipo de associação ao perfil | Escolha o tipo perfil de associação. Por exemplo, para perfil de aplicação escolha o conteúdo. |
| Tipo de objeto do perfil | Escolha o tipo de perfil. |
| Filtro de tipo de objeto | Filtra para o perfil de objetos. O perfil de objetos será inserido. Filtro para o perfil de objetos. Os objetos de perfil serão posicionado sem uma coluna de relatórios. |
| Tipo de objeto | Escolha um tipo de objeto. |
| Filtro de objeto | Filtra para os relatórios de objetos. Você deve usar uma expressão regular para filtrar. |
| Medida | Escolha a unidade dos dados do relatório. |
| Sentido | Escolha o sentido do tráfego. |
| Instante inicial | Escolha o instante inicial do relatório para selecionar os dados. |
| Instante final | Escolha o instante final do relatório para selecionar os dados. |
| Excluir fins-de-semana | Excluir períodos de fins-de-semana do relatório de dados. |
| Intervalo | Se todas as opções estiverem marcadas, este campo será ignorado, senão o dado é selecionado com aquele intervalo para cada dia. |
| Percentual de limite | Escolha essa opção para ter um dado do relatório do tráfego limite configurado em cada objeto. Esta opção irá trabalhar apenas quando a unidade selecionada for bytes, desde que o tráfego limite também esteja em bytes. |
| Formato de saída | Opção disponível apenas para relatórios não-templates. Uma vez que o relatório se torna um template, esta opção é ignorada. |
| Taxa média em Mbps | Mostra a taxa média em Mbps. |
| Use prefixo SI | Use o prefixo SI para mostrar 40.469722M ao invés de 40469722, por exemplo. |

Syslog

Definições

Você pode configurar qualquer dispositivo para enviar mensagens Syslog para o TRAFip.

As mensagens são recebidas pela porta UDP 514.

As mensagens syslog serão armazenadas e deletadas baseadas na configuração de armazenamento syslog.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Syslog** → **Novo relatório** .
2. Preencha o formulário:

Tabela 5.24. Relatório Syslog

| Campos | Descrição |
|------------------|---|
| Início | Escolha o horário para começar e selecione a data. |
| Fim | Escolha o horário para terminar e selecione a data. |
| Origem | Selecione a porta de origem IP ou host para as mensagens syslog. Deixe em branco para ter todos os hosts. |
| Prioridade | Selecione a mensagem prioridade. Deixe 0 para ter todas as prioridades. |
| Mensagem | Filtra a mensagem syslog. Deixe em branco para ter todas as mensagens. |
| Nível | Selecione o nível de mensagem syslog. O padrão é todas as mensagens. |
| Número de linhas | Escolha um limite para a saída do relatório. |
| Formato de saída | Opção disponível apenas para relatórios que não são template. Uma vez que um relatório se torna um template, essa opção é ignorada. |

3. Clique no botão Enviar.

Dados brutos

Definições

Os relatórios de dados brutos fornecem estatísticas detalhadas e consolidadas para todos os fluxos coletados pelo TRAFip.

Quanto mais campos você selecionar, maior e mais detalhado será o seu relatório.


Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatórios** → **Dados brutos** .
2. Escolha a opção **Agendar novo relatório** ou um template da opção **relatórios agendados**.
3. Preencha o formulário:

Table 5.25. Relatório de dados brutos

| Campo | Descrição |
|-----------------------------------|--|
| Gerar relatório Salvar template | Escolha o relatório de uma única execução ou salve um template para salvar um relatório como um template. |
| Formato de saída | Opção disponível apenas para relatório que não é template. Escolha o formato de saída desejado. |
| Número de linhas | Opção disponível apenas para relatório que não é template. Você pode mudar o número máximo de linhas em Sistema → Parâmetros → Relatórios na opção Número máximo de linhas por relatório . |
| Exibir IP das interfaces | Marque esta opção para ter o IP da interface mostrado no relatório quando o campo de interface for selecionado. |
| Início dos dados | Escolha o horário inicial para selecionar os dados brutos. O processo de sumarização roda a cada cinco minutos. Logo, o minuto deve ser preenchido com múltiplos de 5. |
| Tipo de objeto | Tipo de objeto que será usado neste relatório. |
| Objeto | Selecione o objeto para este relatório. Os objetos disponíveis irão depender do tipo de objeto selecionado. |
| Intervalo | Selecione o intervalo do relatório. Ex: Se você selecionar 10 min, o relatório será selecionado do campo Início dos dados mais 10 minutos. |
| Direção | Selecione a direção que o tráfego deve ser filtrado. |
| Ordenar por | Selecione a unidade para ordenar os dados do relatório. |
| Excluir objetos do perfil | Esta opção irá filtrar fora dos objetos do perfil selecionado. Isto é muito útil para achar tráfego indefinido. |
| Tratamento de sampling rate | Escolha se o número de pacotes e bytes dos fluxos devem ser multiplicados pela sampling rate ou configurados pelo dispositivo. Se você escolher a opção de configuração, você deve ir no campo Configuração de sampling rate no formulário de configuração do dispositivo. |
| Sumarização temporal dos fluxos | Marque sim e as entradas do relatório com as mesmas chaves serão resumidas no tempo. Neste caso, o tempo inicial é o tempo inicial do primeiro fluxo, o tempo final é o tempo final do último fluxo e a duração é a diferença entre estes valores. |
| Formatar duração | Marque esta opção para ter uma duração do fluxo formatada em horas, minutos e segundos. |

| Campo | Descrição |
|---------------------|---|
| Campos do Netflow | Escolha o campo do netflow para este relatório. Ele também pode ser editado no relatório gerado e ele será recarregado. |
| Listagem dos fluxos | Marque esta opção para ter todos os fluxos listados. |
| Filtros | Os filtros serão automaticamente preenchidos dependendo da opção do gráfico. Por exemplo, se você selecionar apenas a opção Curva , os filtros irão refletir aquilo. Você também pode adicionar mais filtros ao relatório. |

- No relatório gerado, você pode traduzir: endereço de IP para grupo, endereço de IP para subrede, endereço de IP para nome de host, endereço de IP para netbios, número de AS, fluxos para aplicação, fluxos para ToS e fluxos para grupo de ToS. Além disso, você poderá visualizar um Top 10 dos objetos em forma de gráfico em pizza (para isso, clique no ícone ).
- Clicando no IP de origem ou no IP de destino, será exibida uma animação mostrando o fluxo-a-fluxo do IP selecionado dentro de um período de 5 minutos.

Dica

O banco de dados dos dados brutos é indexado por exportadores de endereços IP, logo se você conhece o dispositivo ou a interface que exportou o tráfego que deseja analisar, você deve emitir o relatório de dados brutos no dispositivo ou interface. Desta forma o relatório será mais rápido e demandará menos recursos do sistema.

Relatório de Projeção

Uma vez que este recurso está ativado, o sistema é capaz de prever o comportamento de qualquer curva de um gráfico e informar a violação de data de um determinado limiar, ou, dada a data, informar o valor da curva.

Configuração

Acesse **Sistema** → **Parâmetros** → **Projeção**

Tabela 5.26. Formulário de configuração de projeção

| Campo | Descrição |
|--------------------|---|
| Graus de liberdade | A ordem polinomial a ser usada. Atualmente, apenas a primeira ordem polinomial é suportada. |
| Amostragem | Configura a amostragem por dia, semana ou mês para o processo de projeção. |
| Histórico | Configura o número de amostras que serão analisadas. Ex: Se você escolher o valor 6 para histórico e semana para amostragem, o sistema irá analisar 6 semanas atrás para prever a projeção. |
| Intervalo | Se a opção Dia todo estiver marcada, este campo é ignorado. Caso contrário, a projeção vai considerar apenas o intervalo configurado para cada dia. |

Habilitando projeção para uma curva gráfica

1. Acesse **Configuração** → **Perfis de tráfego**.
2. Clique no botão Editar para o perfil desejado ou crie um novo.
3. Clique **Sim** na caixa de seleção **Habilitar projeção** e escolha **Sim** em **Usar configurações padrão** ou você pode customizar as configurações para aquela curva.

Importante

O relatório de análise de projeção estará disponível um dia depois de habilitar o recurso, uma vez que o processo de projeção roda em uma base diária.

Relatórios gráficos

1. Acesse o gráfico que contém a curva configurada por projeção, clique com o botão direito nele e selecione a opção **Violação de projeção**.
2. Selecione a curva desejada na caixa de popup, insira um valor para ele e clique OK para ter a taxa de crescimento e a data de violação.

Gerando um novo relatório

1. Acesse **Dados históricos** → **Relatório** → **Projeção** → **Novo relatório** .
2. Preencha o formulário:

Tabela 5.27. Formulário de relatório de projeção

| Campo | Descrição |
|---------------------------------|---|
| Tipo de projeção | Escolha o Perfil de Objeto ou Objeto. |
| Perfil | Selecione o perfil de objeto. |
| Objeto de perfil | Selecione o perfil de objeto. |
| Tipo de objeto | Selecione o tipo de objeto. |
| Filtro de objeto | Filtre pelos objetos associados ao perfil. |
| Formato de saída | Opção disponível apenas para relatórios que não são template. Uma vez que o relatório se torna um template, esta opção é ignorada. |
| Limite de violação Estimativa | Escolhendo Limite de violação , você entrará com um valor e o SLAview irá retornar a data de violação desse valor. Se você escolher Estimativa , você entrará com uma data e um horário e o SLAview irá retornar o valor da curva nesse momento. |
| Entrada de dados | É possível realizar uma operação (Adição ou Subtração) sobre os valores da curva para calcular a projeção. Você ainda pode escolher o tipo de entrada (modo Absoluto ou Relativo [%]). Basta selecionar as opções desejadas e entrar com o valor, em bits/s. |

3. Após preencher o formulário, clique em **Enviar** para gerar o relatório, que mostrará os objetos, a direção, a data estimada ou o valor estimado de violação, o tráfego limite do objeto (em bps) e o quanto foi usado deste limite.

Graph set

O graph set é um relatório gráfico onde você pode visualizar múltiplos gráficos em modo grid na área de visualização dos dados.

Definições

Usuários dos tipos **Operador** e **Configurador** são capazes de gerenciar apenas seus próprios graph sets.

Usuários **administradores** são capazes de visualizar, editar e deletar todos os graph sets, mas não podem criar um graph set para um usuário específico.

Criação

Acesse o caminho **Dados históricos** → **Graph set** → **Novo graph set** .

Tabela 5.28. Criação de graph set

| Campo | Descrição |
|--------------------|---|
| Nome | Nome do graphset. |
| Descrição | Descrição sobre o graphset. |
| Tempo entre slides | Tempo em segundos para mudar os slides utilizados na visualização NOC. |
| Exibir no NOC | Selecione Sim para o gráfico estar disponível no NOC display. |
| Salvar em | Caminho para salvar uma imagem do graphset. Exemplo: C:\Users\Telco\Images |
| Dimensões | Dimensões da imagem salva. |

Adicionando gráficos

1. Acesse qualquer gráfico.
2. Clique no gráfico com o botão direito do mouse.
3. Acesse a opção **Associar a Graph Set** no popup menu e selecione o graph set desejado.

Há uma outra maneira de adicionar gráficos ao graph set. Ela torna possível a adição de gráficos dos tipos barra e pizza. Siga o procedimento abaixo:

1. Acesse o graph set;
2. Clique no símbolo +;
3. Preencha os campos (tipo de objeto, objetos, gráficos, tipo de gráfico e período);

4. Clique em **Inserir gráfico**.

Dica

Para desassociar um gráfico, basta clicar no símbolo **X** ao lado dele.


Visualizando um graph set

1. Acesse o caminho **Dados históricos** → **Graph Set**
2. Clique no ícone para o Graph Set desejado que está na árvore do menu.

Editando um graph set

1. Clique em **Dados históricos** → **Graph set**.
2. Escolha um dos seguintes botões:
 - **Dependências** para deletar gráfico de um graph set.
 - **Editar** para mudar os campos de nome e descrição do graphset.
 - **Deletar** para apagar o graph set.

Gerando gráficos para um graph set

1. Acesse o graph set;
2. Clique no símbolo ;
3. Selecione uma das opções:
 - **Visualizar gráficos** para configurar o tempo de início para os gráficos mostrados na tela.
 - **Salvar imagens** para gerar e salvar cada gráfico como uma imagem no formato PNG.
4. Preencha os campos:
 - **Início dos dados**: Momento de início do gráfico;
 - **Salvar em**: Caminho para salvar uma imagem do graph set. Exemplo: C:\Users\Telco\Images;
 - **Dimensões**: Dimensões da imagem a ser salva.
5. Clique no botão **Gerar gráficos**.

NOC Display

O NOC display é um modo de visualização de Graph sets. Nele, todos os graph sets habilitados pelo usuário alternam-se automaticamente após um período previamente configurado em cada graph set.

Este recurso é de grande utilidade quando o operador deve checar todos os gráficos do graph set constantemente.

Capítulo 6. Configuração

Perfis de tráfego

Definições

Perfis de tráfego te habilitam a construir análises onde o tráfego de certos objetos podem ser discriminados em outros objetos.

Para construir esse tipo de análise, você tem que configurar um perfil, inserir objetos nele e depois associar o perfil a outro objeto.

O banco de dados formado por esta configuração será a base para mostrar o perfil gráfico e relatórios, como o relatório de perfil de tráfego.

Alguns exemplos de análise de perfil são: interface contra aplicações, subredes contra subredes, subredes contra aplicações e assim por diante.

Configuração

1. Acesse **Configuração** → **Perfis de tráfego**.
2. Clique no botão Novo para criar um novo perfil.
3. Preencha o formulário abaixo:

Tabela 6.1. Formulário de perfil de tráfego

| Campo | Descrição |
|----------------------------|---|
| Nome | Nome do perfil |
| Tipo | O tipo de perfil habilitará você a selecionar objetos daquele tipo associado àquele perfil. |
| Curvas de gráfico | Escolha os objetos que vão pertencer a esse perfil e as cores de suas curvas no gráfico. Para isso, arraste os objetos da caixa esquerda para a direita e depois clique no botão Editar cores . |
| Legenda indefinida padrão | Se você quiser renomear a curva Indefinida , selecione Não e preencha o campo Rótulo da maneira que desejar. |
| Projeção | Escolha se você quer habilitar Projeção para alguma curva. Vá à seção Projeção para informações sobre como configurar estes parâmetros. |
| Caixa de seleção de objeto | Use este menu para selecionar os objetos cujo tráfego será analisado por este perfil. Na primeira camada, selecione o tipo de objeto, logo o sistema irá mostrar os objetos disponíveis e, na segunda camada, selecione os tipos de análises. |

Objetos disponíveis

- Aplicação
- Grupo de aplicação
- Grupo de interfaces
- Grupo de sistemas autônomos
- Grupo de subredes
- Grupo de ToS
- Objeto mapeado
- Protocolo
- Sistema autônomo
- Subrede
- ToS

Tipos de análises

O tipo de análise que você seleciona quando um objeto é associado a um perfil irá ditar a forma com que o tráfego será classificado.

Existem três tipos de análises disponíveis, as quais serão explicadas a seguir.

Matriz

Os objetos do perfil de tráfego são procurados na direção oposta ao tráfego que está sobre análise.

Por exemplo, vamos supor que um perfil de tráfego composto por subredes é associado a uma subrede abaixo deste tipo de análise. Depois, para o tráfego de destino de subrede, o TRAFip irá tentar igualar as subredes do perfil de tráfego contra o campo de origem IP. Para o tráfego de origem de subrede, o TRAFip irá tentar igualar o perfil de tráfego contra o campo de IP de destino.

Este tipo de associação de perfil habilita a análise do tráfego trocado entre um escritório central e um escritório regional da empresa, por exemplo.

Para implementar esta análise, siga os procedimentos abaixo:

1. Crie uma subrede para cada escritório regional e uma subrede para o escritório central.
2. Crie um perfil de tráfego contendo as subredes do escritório regional.
3. Associe um perfil de tráfego à subrede do escritório central usando o tipo de análise **Matriz**.

Distribuição

Os objetos do perfil de tráfego são procurados na mesma direção do tráfego que está sob análise.

Por exemplo, vamos supor que um perfil de tráfego composto de subredes é associado a uma subrede sob esse tipo de análise. Depois, para o tráfego de destino de subrede, o sistema irá tentar igualar as subredes do perfil de tráfego contra o campo de destino IP. Para o tráfego de origem de subrede, o sistema irá igualar as subredes do perfil de tráfego contra o campo IP de origem.

Este tipo de associação de perfil habilita análises de como detalhar tráfego de entrada e saída de um grupo de subredes. Isto é útil, por exemplo, para checar o balanceamento de um grupo de servidores.

Para implementar esta análise, siga os procedimentos abaixo:

1. Criar uma subrede para cada servidor.
2. Criar um grupo de subrede contendo servidores de subrede.
3. Criar um perfil de tráfego contendo servidores de subredes.
4. Associar o perfil de tráfego ao grupo de subrede usando o tipo de análise de distribuição.

Conteúdo

O tipo de análise de conteúdo é usado por objetos, onde não existe noção a respeito do tráfego de origem ou destino.

Estes objetos são, por exemplo, protocolos, aplicações e ToS. Assim, para cada fluxo, existe apenas um protocolo, uma aplicação e um ToS.

Sempre que você criar perfis com este tipo de objeto, use o tipo de análise de conteúdo.

Domínios

Este objeto permite que todos os objetos, exceto dispositivos, interfaces e grupos de interfaces sejam sumarizados, considerando apenas o fluxo de cada domínio.

Domínios são geralmente usados para separar fluxo de tráfego similar através dos diferentes roteadores. Ex: roteadores de borda e roteador de backbone.

Para trocar de domínio, use a caixa de seleção que aparece na aba **Dados Históricos** com cada nome de domínio.

Definições

- Um domínio é composto de dispositivos.
- Um dispositivo pode apenas ser associado a um domínio.
- Tráfego domínio total: composto pelo somatório de todos os fluxos pertencentes aos dispositivos de domínio.

Configuração

Para criar um novo domínio, acesse **Configuração** → **Domínios** e clique no botão Novo.

Tabela 6.2. Formulário de Domínio

| Campo | Descrição |
|-------------------------------|---|
| Nome | Entre com um nome para o domínio. |
| Intervalo entre alarmes (seg) | Somente será emitido um alarme do mesmo tipo (de alarme) após este período ter passado, em relação a uma ocorrência prévia. |

| Campo | Descrição |
|--|---|
| Limite de tempo para acumular tráfego (seg) | Esse limite define o período em que as análises ocorrem. No caso, somente serão considerados os dados com diferença de tempo entre o primeiro e o último que fiquem dentro deste limite. |
| Threshold em Bytes (acumulado no período) | Limite de bytes recebidos/enviados por/para um host para ativar um alarme. Um alarme de tráfego suspeito do tipo <u>Alto fluxo de dados entre dois IPs</u> será ativado caso esse limite seja atingido. |
| Threshold em Pacotes (acumulado no período) | Limite de pacotes recebidos/enviados por/para um host para ativar um alarme. Um alarme de tráfego suspeito do tipo <u>Alto fluxo de dados entre dois IPs</u> será ativado caso esse limite seja atingido. |
| Threshold em Fluxos (acumulado no período) | Limite de fluxos recebidos/enviados por/para um host para ativar um alarme. Um alarme de tráfego suspeito do tipo <u>Alto fluxo de dados entre dois IPs</u> será ativado caso esse limite seja atingido. |
| Threshold para IP Flood (IPs acumulados no período) | Limite de conexões recebidas/feitas por/para um host. O valor mínimo é 2 para que um alarme seja ativado. |
| Porcentagem mínima para caracterização de tráfego | Quando em arquitetura distribuída, pode-se definir que o tráfego seja caracterizado como suspeito nas coletoras quando apenas uma porcentagem do total dos thresholds for atingida. Defina essa porcentagem mínima usando este campo. |
| Tolerância de diferença entre horário local e do exportador | Defina o tempo de tolerância, em segundos, para considerar que um dado fluxo está dentro do período sendo analisado e não ser descartado. O valor mínimo deve ser 60 . |
| Lista de IPs excluídos da análise de tráfego suspeito (IP/máscara) | Entre com os endereços IP das subredes a serem excluídas da análise de tráfego suspeito. Separe por vírgulas. |
| Agrupamento para grupo de interfaces | Selecione os agrupamentos para grupos de interface que farão parte do Domínio. |
| Dispositivos do domínio | Selecione os dispositivos que vão compôr o Domínio. |

Uma vez que o domínio é criado, você deve configurar a Interface RFI dependendo da sua topologia de rede.

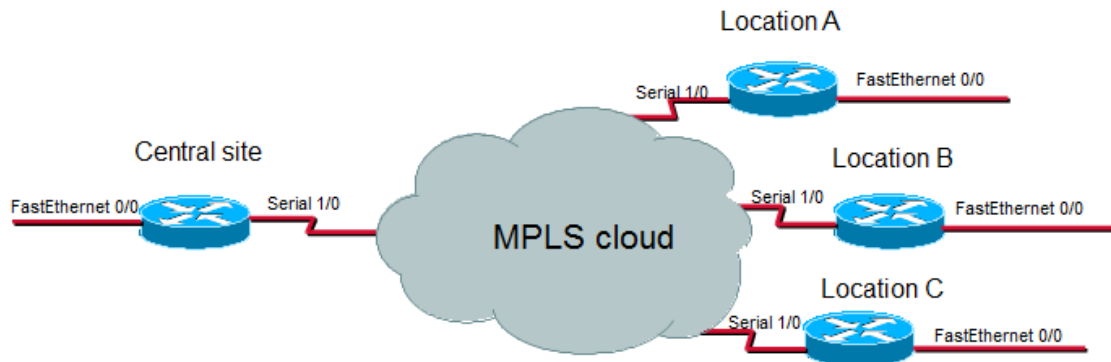
Interfaces RFI

A configuração RFI irá fazer o sistema filtrar o mesmo tráfego exportado por mais de um roteador em um domínio.

Este filtro é baseado no campo de entrada de interface, logo não será usado por interfaces, grupos de interfaces e dispositivos.

Todos os fluxos são gravados em disco, logo o filtro será usado apenas quando o sistema sumariza o tráfego ou para relatórios de dados brutos. O filtro não irá prevenir o recebimento de fluxos.

O exemplo abaixo ilustra o cenário onde o filtro RFI é necessário. Para análise correta deste cenário, é necessário que todos os roteadores exportem fluxo em todas as interfaces.



Exemplo de interface RFI

O que acontece é que quando um fluxo de pacotes de um site central para uma localização remota, ele é exportado duas vezes. Uma vez ele entra no roteador do site central e outra vez ele entra no roteador de uma localidade.

Para sumarização correta da subrede do site central, por exemplo, apenas um dos fluxos deve ser considerado.

Se todas as interfaces LAN, neste caso, as interfaces FastEthernet, são configuradas como interfaces RFI, os fluxos exportados possuindo essas interfaces como entrada não serão considerados, portanto, o resultado final da sumarização estará correto.

O TRAFip pode configurar automaticamente as interfaces RFI, considerando que todas as interfaces na mesma máscara de rede de 30 bits estão conectadas a cada uma e definidas como RFI. Esta descoberta é realizada utilizando o protocolo SNMP e as interfaces a serem consideradas devem ser marcadas como auto rfi.

Configuração

Acesse **Configuração** → **Domínios** e clique no botão Interfaces RFI para o domínio que você deseja configurar a interface RFI.

Coletoras

Esta seção deve ser usada se você estiver implantando o sistema do modo de arquitetura distribuída.

Para mais detalhes de implantação de arquitetura distribuída consulte a seção de arquitetura distribuída.

Tabela 6.3. Formulário de coletoras

| Campo | Descrição |
|-------|--|
| Nome | Nome para identificar um appliance coletor. |
| Chave | Preencha uma chave com string. Esta string deve ser igual ao campo chave de coletor no menu Sistema → Parâmetros → Arquitetura distribuída no appliance coletor. |

| Campo | Descrição |
|--------------------|--|
| Endereço de IP | Endereço de IP que o coletor irá usar para acessar o appliance central. |
| IP do exportador | Endereço de IP usado pelo coletor para receber fluxos do roteador. Este endereço de IP é usado em caso de querer que o sistema reconfigure automaticamente a exportação de netflow no roteador se um appliance coletor falhar. |
| Senha | Esta senha deve corresponder ao campo senha no menu Sistema → Parâmetros → Arquitetura distribuída no appliance coletor. |
| Coletora de backup | Coletora que irá ser o backup para esta coletora em caso de falha. |
| Dispositivos | Dispositivos que esta coletora irá coletar. |

Importando arquivos de coletoras

Para importar um arquivo de coletoras, acesse **Configuração** → **Coletoras**.

Clique no botão de importar e carregue o arquivo.

Um arquivo de dispositivo importado possui os seguintes campos:

Tabela 6.4. Campos de arquivos de coletoras

| Campo | Descrição |
|----------------|---|
| Nome | Possíveis caracteres para o campo nome. |
| Chave | Caracteres alfanuméricos. |
| Endereço de IP | Endereço de IP. Ex.: 10.0.0.1 |
| Senha | Possíveis caracteres para campo de senha. |

Objetos

Nesta tela você pode acessar cada forma de configuração de objeto e os objetos já configurados.

Para alguns tipos de objetos, você tem a opção de fazer um upload de um arquivo de configuração para configurar vários objetos.

Importando arquivos de objetos

1. Acesse **Configuração** → **Objetos** e clique no botão Importar para o tipo de objeto desejado.
2. Faça o upload de um arquivo formatado de acordo com as instruções na tela.
3. Clique no botão Adicionar.
4. Ajuste as configurações e clique no botão Salvar.

Mapeadores

Mapeadores são usados para descobrir objetos relacionados utilizando o protocolo SNMP ou por scripts. Exemplos daqueles objetos são: interface de rede, processadores, bancos de memória, unidades de storage, probes e outros.

Mapeadores podem ter dispositivos associados automaticamente a eles, considerando Regras que devem ser selecionadas como condição

Procedimento 6.1. Criando um mapeador

1. Selecione **Configuração** → **Mapeadores**.
2. Clique no botão Novo item e preencha o formulário como detalhado abaixo:

Table 6.5. Formulário de Mapeador

| Campo | Descrição |
|--|--|
| Nome | Nome do mapeador |
| Ícone | Imagem que será mostrada próxima aos objetos descobertos por este mapeador na árvore do menu. Veja o passo 3 para instruções de customização dessa imagem. |
| Remoção automática | Se você quer que os objetos mapeados por este mapeador sejam removidos depois de um certo número de dias consecutivos que eles estão perdidos, selecione Sim e preencha o número de dias. |
| Incluir prefixo | Inclui o nome do mapeador como prefixo para os objetos descobertos por este mapeador. |
| Instância da OID usada como nome de objeto | Marque esta opção se ao invés de preencher o nome do objeto com o valor da OID, o mapeador deve preenchê-lo com o valor da instância da OID. Esta opção deve ser utilizada por objetos que não tenha uma OID cujo valor pode representá-los. Logo você pode utilizar uma OID estatística e um mapa de instância de objetos com esta opção. |
| Nome | Nome da OID a ser usada para o mapeamento de objetos. |
| OID | OID que será utilizada. |
| MIB | OID MIB. |
| Filtro por coletora SNMP | Filtra pela resposta da coletora SNMP. |
| Associação de dispositivos | Habilita associação de dispositivos automáticos ao mapeador considerando as Regras. Quando habilitado, o formulário irá mostrar a opção remoção automática que irá remover os dispositivos associados quando as condições não forem mais conhecidas. |

| Campo | Descrição |
|--------------|---|
| Dispositivos | Selecione os dispositivos associados ao mapeador. |

Dica

Abaixo da seção Configuração de Mapeamento, você deve especificar a OID (Object Identifier) de uma MIB (Management Information Base) onde o sistema pode achar nome de instâncias únicas como valores retornados, logo o objeto pode ser identificado. Esta OID pode ser carregada utilizando a ferramenta MIB Browse clicando no botão procurar OID.

Use o botão Encontrar OID para pesquisar a MIB e preencher os últimos campos do formulário.

3. Configurando os ícones de mapeador.
 - a. Selecione no menu **Configuração** → **Mapeadores** e clique no botão Mudar ícones.
 - b. Clique no botão Novo ícone.
 - c. Preencha o nome do mapeador e faça um upload de um ícone para cada condição de objeto.
 - d. Clique no botão Enviar.

Mapeamento cruzado de OIDs

Este recurso permite que você crie um mapeador especificando 2 OIDs. O mapeador irá encontrar o valor para a primeira OID e depois usará como index para achar o valor da segunda OID.

Logo, o mapeador irá mapear o index da primeira OID com o valor da segunda OID.

Este mapeador pode ser usado, por exemplo, para mapear CPUs Cisco, onde você pode especificar as seguintes OIDs:

1.3.6.1.4.1.9.9.109.1.1.1.1.2;1.3.6.1.2.1.47.1.1.1.1.7

A primeira OID é a `cpmCPUTotalPhysicalIndex` do `CISCO-PROCESS-MIB` e a segunda é a `entPhysicalName` do `ENTITY-MIB`, onde você pode achar o nome de cada CPU.

Associando dispositivos aos mapeadores

Depois de configurar um novo mapeador, você deve associá-lo a um dispositivo onde o objeto deve ser descoberto. Esta associação pode ser feita em cada configuração de dispositivo ou clicando no botão Associação de dispositivos na lista de mapeadores.

Exportando e importando mapeadores

O botão **Exportar** exporta toda configuração do mapeador para um arquivo. Para importar essa configuração de volta, você pode utilizar o botão **Importar** e então fazer download desse arquivo.

EPM (Extended Processing Module)

EPM é outra aplicação em adição ao já existente instalado no cliente. É um módulo estendido da solução de monitoramento.

Necessita ser habilitado em **Sistema** → **Parâmetros** → **EPM** .

EPM é uma solução escalável para os vários usuários acessando o sistema pela interface web, visualizando gráficos e relatório de dados sumarizados. Os dados sumarizados são replicados para as máquinas EPM realizando um acesso de dados mais rápido e dados redundantes.

1. Clique **Configuração** → **EPM**.
2. Clique em Novo para criar uma nova entrada EPM.
3. Preencha os campos nome e endereço IP.
4. Selecione status administrativo.
5. Clique em Salvar.

Regras

Criação de regras

1. Selecione **Configuração** → **Regras** e selecione o tipo de regra, se é dispositivo ou objeto mapeado.
2. Clique no botão Novo para criar uma nova regra e preencha o formulário:

Tabela 6.6. Perfil automático de regras

| Campo | Descrição |
|------------------------------------|---|
| Nome | Nome da regra. |
| Descrição | Descrição da regra. |
| Filtro por campos da base de dados | Filtro baseado nos campos da base de dados. Por exemplo, o campo Nome refere-se ao nome do objeto e o campo Mapeador (somente para regras de objeto mapeado) refere-se ao nome do mapeador. |
| Filtro por coleta SNMP | Filtra baseado nas OIDs que serão monitoradas quando as regras forem testadas. Selecione a opção Usar índice de objeto mapeado quando usando OIDs que devem ser testadas contra objetos mapeados, como, por exemplo, ifConnectorPresent. |

Filtro 'No Response'

O filtro de verificação de resposta, que está localizado no 'Filtro por coleta SNMP', consiste em validar um objeto no caso de retornar uma mensagem específica de erro.

Para utilizá-lo, você deve escolher o operador 'No Response' no filtro. No campo 'valor' você deve utilizar um desses valores:

- \$nosuchobject\$ - É utilizado para validar a resposta 'Sem tal objeto' de um objeto.
- \$nosuchinstance\$ - É utilizado para validar a resposta 'Sem tal instância' de um objeto.

Credencial de dispositivo

Muitos dispositivos utilizam as mesmas configurações de SNMP e de acesso remoto.

É possível configurar estes parâmetros em uma credencial e depois associá-la aos dispositivos que possuem a mesma configuração.

Para criar uma nova credencial, acesse **Configuração** → **Credencial de dispositivo** → **Nova credencial de dispositivo** ou **Configuração** → **Credencial de dispositivo** → **Credencial de dispositivo** e clique no botão **Novo**.

Tabela 6.7. Formulário de Credencial de dispositivo

| Campo | Descrição |
|------------------|--|
| Nome | Defina o nome da credencial. |
| Protocolo | Defina se a credencial será de SNMP , SSH ou Telnet . |
| Versão do SNMP | Selecione a versão SNMP. Os possíveis valores são: SNMP v1 ou SNMP v2c Especifica uma community SNMP SNMP v3 Especifica o tipo de autenticação e seus parâmetros |
| Community SNMP | Preencha a community SNMP. |
| Porta SSH | Preencha a porta SSH. O valor padrão é 22 . |
| Porta Telnet | Preencha a porta Telnet. O valor padrão é 23 . |
| Usuário | Usuário para ser usado para acessar o dispositivo. Esta string está disponível como um campo livre %username% para scripts de provisionamento. |
| Senha do usuário | Senha do usuário que irá acessar o dispositivo. Esta string está disponível como um campo livre %passwd% para scripts de provisionamento. |
| Senha de enable | Senha de enable é a usada para acessar o dispositivo. Esta string está disponível como um campo livre %enable_passwd% para scripts de provisionamento. |
| Dispositivos | Associe os dispositivos que devem utilizar a credencial. |

Capítulo 7. Ferramentas

Software externo

Telcomanager Windows Collector

Faça o download do executável **Telcomanager Windows Collector** para instalar o coletor de Netflow para Windows.

Ele encaminha todos os pacotes de Netflow recebidos por uma máquina Windows para um appliance com TRAFip.

Telcomanager Host Agent

Faça o download do executável **Telcomanager Host Agent** (THA) para instalar este agente no Windows.

Este agente coleta informações acerca dos processos rodando.

Discovery

O recurso Discovery é usado para descobrir todos os hosts que estão sendo usados numa rede. Preencha o campo IP/Máscara e clique em Executar para iniciar a função discovery.

Quando o processo termina, o sistema irá mostrar uma lista com todos os hosts descobertos.

Capítulo 8. Sistema

Registro de acesso

Acesso de usuário

Esta opção mostra um relatório sumarizado por dia contendo o registro de acesso de usuários. Cada linha do relatório é um link para um relatório diário detalhado.

Acesso simultâneo

Este relatório mostra o número de usuários que estão logados no sistema para cada grupo de usuário.

Backup/Restore

Você pode executar backup e restore de todos os dados do sistema de qualquer servidor ftp ou um simples arquivo download/upload com todas as configurações do sistema.

Vá em **Sistema** → **Backup/Restore** para trabalhar com as seguintes opções de backup/restore:

Backup local de configuração

Clique neste ícone para mostrar todos os arquivos de backup de configuração.

Você pode criar um novo arquivo clicando no botão Criar novo.

O botão Configurar é usado para selecionar o número de arquivos a serem mantidos.

Clique no botão Download para fazer o download de um arquivo de configuração para o seu desktop.

O botão Copiar para Restore é usado para copiar o arquivo de configuração para a área de restore para que ele possa ser restaurado.

Restore local de configuração

Esta opção é usada para restaurar um arquivo de backup. Fazendo isto, todas as configurações atuais do sistema serão substituídas pelas definições contidas no arquivo restaurado.

Para executar uma restauração do sistema, você deve fazer upload do arquivo de configuração da sua máquina local ou copiar um arquivo de backup antigo disponível no sistema e depois clicar no botão Restore para aquele arquivo.

Backup remoto

Esta opção pode ser usada para salvar os arquivos de configuração e dados históricos do sistema em um servidor de backup remoto.

Tabela 8.1. Formulário de backup remoto

| Campo | Descrição |
|--------------------------------|--|
| Versão do IP | Escolha se é IPv4 ou IPv6. |
| Servidor de backup | Endereço de IP do servidor de backup. |
| Diretório de backup | Diretório no servidor de backup. |
| Usuário | Usuário para ser autenticado no servidor de backup. |
| Senha do usuário | Senha. |
| Protocolo utilizado no backup | Protocolo a ser usado nos backups. |
| Porta utilizada pelo protocolo | Número da porta. |
| Tamanho do servidor (GB) | Tamanho do servidor em Gigabytes. |
| Ativar backup | Selecione Sim para ativar o recurso de backup. |
| Hora para realizar o backup | Selecione o instante do dia para a execução dos backups. |

Importante

Este recurso não irá salvar o fluxo de dados brutos, já que estes dados são mais usados para solucionar problemas e usualmente precisam de volume grande de espaço de armazenamento.

Restore remoto

Selecione um único sistema para executar restore de dados ou clique Requisitar restore completo para buscar dados de todos os sistemas.

Importante

- O servidor ftp deve estar online, já que os dados serão buscados nele.
- Apenas execute esta operação em uma instalação de um TRAFip ou SLAview novos e vazios, já que todos os dados serão substituídos.

Situação da restauração

Esta opção irá mostrar o status de restauração uma vez que for solicitada uma operação de restauração remota.

Parâmetros

Esta seção é usada para configurar vários parâmetros do sistema que são usados por diferentes processos.

Active directory

Esta opção possibilitará que os usuários loguem no TRAFip usando o método de autenticação Active Directory Kerberos.

Para um usuário ser autenticado por esse método, é preciso que o TRAFip esteja configurado.

Tabela 8.2. Formulário de Active directory

| Campo | Descrição |
|--|---|
| Habilitar autenticação pelo Active Directory | Uma vez que a opção Sim estiver selecionada, o campo Autenticação local aparecerá no formulário de usuário. |
| Servidor | Digite o endereço do servidor Active Directory. Exemplo: kerberos.example.com |
| Domínio | Digite o domínio do Active Directory. Exemplo: ATHENAS.MIT.EDU |

Quando este método está ativado, não existe autenticação local, ou seja, qualquer usuário que não seja do tipo **Administrador** loga pelo TACACS.

Importante

O usuário **Administrador** tem a opção de escolher logar localmente ou não, entretanto, recomenda-se que haja sempre uma conta de **Administrador** com **Autenticação local** ativada, caso seja utilizado controle de acesso externo.

Agentes de associação

Agente de associação automática de mapeadores

Configure os períodos desejados para que a associação automática de mapeadores seja executada. Isso acontecerá em dois momentos do dia.

Tabela 8.3. Formulário de agente de associação automática de mapeadores

| Campo | Descrição |
|------------------------------|---|
| Primeiro horário de execução | Escolha o horário para a primeira execução acontecer. |
| Segundo horário de execução | Escolha o horário para a primeira execução acontecer. |

Análise de ameaças

Nesta seção, você configurará se deseja utilizar o mecanismo de análise de tráfego suspeito do TRAFip ou o módulo de detecção de ameaças, TRAFwatcher.

Tabela 8.4. Formulário de parâmetros da Análise de ameaças

| Campo | Descrição |
|--|---|
| Período máximo de armazenamento de Tráfegos suspeitos (dias) | Configure o máximo período de tempo, em dias, em que os eventos de tráfego suspeito ficarão armazenados no sistema. |
| Usar o mecanismo legado de análise de ameaças | Selecione Sim para usar o mecanismo de tráfego suspeito do TRAFip. Caso contrário, a análise de ameaças será feita pelo TRAFwatcher. |

Importante

Ao usar o módulo TRAFwatcher, é necessário habilitar a análise de ameaças no formulário de cada subrede desejada.

Armazenamento de dados

Nesta área, você deve configurar o armazenamento de espaço que deveria ser alocado para cada tipo de dado do sistema.

O campo **Espaço de distribuição disponível** irá mostrar o espaço que ainda pode ser distribuído.

Para checar quanto espaço cada área está consumindo, você deve fazer login no sistema desejado (TRAFip, SLAview ou CFGtool) e acessar **Sistema** → **Diagnósticos** → **Armazenamento de dados**. O item do banco de dados TDB corresponde aos dados sumarizados para cada tipo de sistema.

Você pode realizar a redistribuição de espaço de armazenamento entre diferentes áreas a qualquer momento.

Tabela 8.5. Formulário de armazenamento de dados

| Campo | Descrição |
|--|--|
| Iniciar processo a partir da ocupação em % | Quando este valor for atingido, o processo de limpeza será executado de acordo com o tipo de execução configurado. Preencha um valor entre 1 e 85 . |
| Tipo de execução | Escolha se o agente rodará a cada Intervalo de tempo ou num Horário agendado . |
| Intervalo de tempo para execução (minutos) | Defina o intervalo de tempo, em minutos, para a execução do agente. O valor mínimo é 10 . |
| Horário de execução | Defina o horário em que a execução do agente acontecerá. |
| Espaço disponível para os arquivos de SYSLOG | Armazenamento dedicado para dados brutos de arquivos SYSLOG. |
| Espaço disponível para os arquivos de Relatórios agendados | Armazenamento dedicado para relatórios agendados. |
| Trap receiver storage | Armazenamento dedicado para arquivos de Trap receiver. |
| Espaço disponível para arquivos de captura | Armazenamento dedicado para arquivos de captura. |
| Dados brutos do TRAFip | Área de armazenamento destinada aos arquivos de dados brutos do TRAFip. Este armazenamento normalmente cresce muito mais rápido que os dados sumarizados. Dessa forma, se você configurar com o mesmo tamanho dos dados sumarizados, você terminará com 10 vezes menos dados históricos. |
| Dados sumarizados do TRAFip | Armazenamento dedicado para o TRAFip, dados processados ou TDB - Telco database. Este dado é usado para gráficos e relatórios TOPN. |
| Arquivos de sumarização remota do TRAFip | Armazenamento dedicado para os dados processados do TRAFip enviados pelos coletores num ambiente de arquitetura distribuída. |

| Campo | Descrição |
|--|--|
| Dados de alteração de comportamento do TRAFip | Armazenamento dedicado para os dados de alteração de comportamento, como dados de alarmes históricos, por exemplo. |
| Dados brutos do SLAview | Armazenamento dedicado para dados brutos do SLAview. Isto é, em geral, das coletas SNMP das OIDs. |
| Dados sumarizados do SLAview | Armazenamento dedicado para dados processados pelo SLAview. Este dado é usado para gráficos e relatórios. |
| Arquivos de sumarização remota SLAview | Armazenamento dedicado para os dados processados para os arquivos dos dados SLAview enviados pelos coletores em um ambiente de arquitetura distribuída. |
| Dados de alteração de comportamento do SLAview | Armazenamento dedicado para os dados de alteração de comportamento, como dados de alarmes históricos, por exemplo. |
| Dados de versões do CFGtool | Armazenamento dedicado para versões de configurações dos dispositivos. Mesmo que este valor seja ultrapassado, os dados de versão de dispositivos com apenas uma versão não serão excluídos. |

Quando os campos **Dados brutos (MB)** e **Dados sumarizados (MB)** estão preenchidos com '0' (zero), isso significa que o sistema está distribuindo de maneira automática o **Espaço disponível para distribuição** entre os **Dados brutos do TRAFip**, **Dados brutos do SLAview**, **Dados sumarizados do TRAFip** e **Dados sumarizados do SLAview**.

Você pode configurar manualmente esses valores, mas não se esqueça que os dados brutos tendem a crescer muito mais rápido do que os dados sumarizados. Para redistribuir os espaços, divida o valor de **Espaço disponível para distribuição** por 4. Assim, você terá o valor de cada espaço.

Cuidado

Se você reduzir o espaço de armazenamento de qualquer uma dessas áreas, a próxima vez que o coletor de lixo for executado, ele limpará os dados para adequar o espaço de armazenamento.

Arquitetura distribuída

Estes parâmetros devem ser usados se você desejar rodar o sistema no modo de arquitetura distribuída.

Para mais detalhes da arquitetura distribuída vá à seção arquitetura distribuída.

Tabela 8.6. Formulário dos parâmetros da arquitetura distribuída

| Campo | Descrição |
|---|--|
| Número máximo de falhas consecutivas do coletor | Este número representa quantas vezes o nó da central irá esperar os arquivos processados de um nó do coletor enquanto este nó é considerado desativado. Esta checagem é realizada a cada 5 |

| Campo | Descrição |
|-----------------------------------|--|
| | minutos por um processo de controle para os sistemas TRAFip e SLAView. Depois que o coletor está definido como desabilitado pelo nó central, o coletor de backup, se estiver definido, irá substituir as operações com os coletores defeituosos. |
| Habilitar arquitetura distribuída | Selecione esta opção se o appliance será parte de um sistema de arquitetura distribuída. |
| É coletora? | Marque Sim nesta opção se o appliance terá o papel de coletora no sistema. Caso contrário este appliance será considerado um nó central. |
| Chave do coletor | Preencha com uma string de identificação para identificar este coletor no nó central. |
| Versão do IP | Escolha se é IPv4 ou IPv6. |
| IP da consolidadora | Preencha com o endereço IP do appliance para ser usado como nó central. |
| Senha | Senha usada para autenticação. |

Aviso de Expiração

Configure quantos dias antes da expiração da licença você será lembrado a respeito dela.

Tabela 8.7. Formulário de aviso de expiração

| Campo | Descrição |
|----------------------------|--------------------------------|
| Alertar expiração faltando | Defina um valor entre 10 e 30. |

Backup

- Dados: Parâmetros para executar backup remoto. Veja a seção backup remoto.
- Configuração: configure o número de antigas configurações de backup de arquivos para manter no sistema.

Cisco WAAS

Cisco WAAS (Wide Area Application Services) é uma ferramenta desenvolvida pela Cisco que é capaz de acelerar as aplicações da mesma.

Tabela 8.8. Formulário de Cisco WAAS

| Campo | Descrição |
|---------------------------------------|------------------------------------|
| Habilitar monitoramento ao Cisco WAAS | Escolha Yes ou Não . |

Configuração de HTTPS

Configure o modo HTTPS (HyperText Transfer Protocol Secure).

Tabela 8.9. Formulário de HTTPS

| Campo | Descrição |
|-----------------|--|
| Habilitar https | Escolha Sim e o servidor será reiniciado no modo HTTPS. |
| Certificado | Importe o certificado https. |

Configuração do agente de captura

Configure o número permitido de agentes em execução simultânea.

Tabela 8.10. Formulário de configuração do agente de captura

| Campo | Descrição |
|--|---|
| Número de agentes em execução simultânea | Entre com um inteiro menor ou igual a 10. O valor padrão é 3. |

Configuração regional

Tabela 8.11. Formulário de configuração regional

| Campo | Descrição |
|---|---|
| Separador de decimal | Separador decimal para relatórios do sistema. |
| Linguagem do sistema | Escolha a linguagem padrão do sistema. Cada usuário pode definir sua própria configuração de idioma em configuração do usuário. |
| Número de casas decimais nos arquivos de exportação | Configuração usada para formatar campos de números nos relatórios exportados. |
| Separador de arquivo CSV | Separador para relatórios CSV. |

EPM

EPM (Extended Processing Module) é outra aplicação em adição à já instalada no equipamento. É um módulo estendido da solução de monitoramento.

Tabela 8.12. Formulário EPM

| Campo | Descrição |
|---------------|--|
| Habilitar EPM | Selecione esta opção se você desejar habilitar o módulo de solução de monitoramento. |
| É EPM? | Marque Sim nesta opção se esta aplicação for utilizada como EPM. |

Importante

Mudando esta configuração você irá perder todos os seus dados históricos, logo, tenha cuidado!

Filtro simples

Este filtro mostra-se muito útil para os usuários do sistema quando há uma quantidade considerável de grupos de subrede. Ao escolher o **número de caracteres do filtro de Subredes**, aparece um filtro no

menu principal da seção **Dados históricos** → **Subredes** onde aparecem todos os grupos de subredes, mas apenas com a quantidade de caracteres delimitadas por você.

Assim, quando você selecionar um desses grupos mostrado no filtro, na seção **Grupos de subredes** só aparecerão o grupo escolhido e os posteriores a ele.

É importante lembrar que, ao configurar o filtro simples, o menu de subredes deixa de ser mostrado. Logo, as subredes só poderão ser visualizadas através dos grupos.

Importante

Quando esse campo está configurado como **0** (zero), não há a existência desse filtro.

Grafador

Ajuste dos parâmetros do grafador

Tabela 8.13. Formulário de parâmetros do grafador

| Campo | Descrição |
|---|--|
| Habilitar gráfico derivativo como padrão? | No modo padrão, pontos de gráficos são conectados usando interpolação linear. No modo derivativo, a interpolação por partes é utilizada. |
| Habilitar atualização automática | Selecione esta opção para ter todos os gráficos atualizados automaticamente. Você também pode habilitar esta opção em tempo de execução para cada gráfico. |
| Mostrar horário comercial | Habilitando essa opção, o horário comercial definido em Preferências locais será mostrado nos gráficos. |
| Excluir fins-de-semana | Habilitando essa opção, os dias do fim de semana serão mostrados com cor mais clara nos gráficos. |
| Intervalo de atualização | Intervalo entre as atualizações. |

Histórico de configuração

Selecione o período de armazenamento para diferentes áreas de configuração.

Tabela 8.14. Parâmetros de históricos de configuração

| Campo | Descrição |
|--|--|
| Período máximo de armazenamento de histórico de configuração | Isto inclui todas as mudanças de configuração, exceto para o usuário relacionado às operações. Este dado será mostrado em Sistema → Diagnósticos → Logs de configuração . |
| Período máximo de armazenamento de histórico de configuração de usuários | Isto é específico para operações de usuário. Estes dados podem ser mostrados em Sistema → Diagnósticos → Logs de configuração selecionando a opção usuário no campo Tipo de objeto . |

| Campo | Descrição |
|---|---|
| Período de armazenamento de máxima estatística de fluxo (meses) | Este campo é relacionado apenas ao fluxo processado. Esta estatística pode ser visualizada em Sistema → Diagnósticos → Estatísticas de fluxo . |
| Período máximo de armazenamento de estatísticas de sumarização | Isto é relacionado apenas ao processo de sumarização. Esta estatística pode ser checada em Sistema → Diagnósticos → Sumarizador . |

Integridade de segurança

Selecione o período de tempo em que o alarme de Integridade de Segurança permanecerá ativo.

Tabela 8.15. Integridade de Segurança

| Parâmetro | Descrição |
|---------------------------------|---|
| Limite de modificação(segundos) | Período de tempo em que o alarme de modificação de arquivos permanecerá alarmado. |
| Limite de alteração(segundos) | Período de tempo em que o alarme de ausência de arquivos permanecerá alarmado. |

Login automático

Este recurso habilita a autenticação bypass para requisições URL vindas de outro sistema.

Para habilitar este recurso, siga o procedimento abaixo:

1. Vá até **Sistema** → **Parâmetros** → **Login automático** .
2. Selecione sim na opção **Habilitar login automático**.
3. Preencha a URL no formato requerido, que é a página cujas requisições serão originadas.
4. No seu servidor web, preencha a seguinte URL: http://TelcoApplianceIP.

Logotipo

Escolha um arquivo de imagem do seu Desktop e faça o upload, logo a imagem será mostrada no canto direito superior.

Lembre que a imagem deve estar com altura fixada em 43 pixels e largura variável de 20 à 200 pixels.

Mapeador de objetos

Para mais detalhes sobre mapeamento de objetos vá à seção configuração de mapeadores.

Tabela 8.16. Formulário de configuração de parâmetros de mapeador de objetos

| Campo | Descrição |
|-----------------------------------|--|
| Intervalo de execução do mapeador | Programe o intervalo entre as execuções do mapeador. |

| Campo | Descrição |
|--|---|
| Período máximo de armazenamento do histórico de configuração | Programe o período de armazenamento de logs pelas configurações realizadas pelo mapeador |
| Limite de mapeadores TCS simultâneos | Defina um limite de execuções simultâneas de mapeadores do tipo TCS. Preencha um valor entre 1 e 200 . A configuração deste parâmetro poderá afetar a performance do sistema, então seja cuidadoso. |

Nível de log

Escolha o nível do ALARMDaemon: **Baixo**, **Médio** or **Alto**.

Este nível determinará a quantidade de detalhes no log do alarme.

Personalização de interface

Você pode customizar a maneira como os dispositivos serão mostrados no menu em árvore em **Dados históricos** → **Dispositivos** → **Dispositivo** .

Para isso, basta preencher o campo **Fórmula de nome de dispositivo** com o que você deseja que apareça no menu.

A fórmula possui tags especiais que utilizam as informações preenchidas nos formulários dos dispositivos. São as seguintes:

Tabela 8.17. Fórmula de nome de dispositivo

| Tag | Descrição |
|------------|--|
| %n | Refere-se ao nome do dispositivo. |
| %a | Refere-se ao endereço de IP do dispositivo. |
| %t | Refere-se ao tipo do dispositivo. |
| %m | Refere-se ao fabricante do dispositivo. |
| %d | Refere-se ao tipo de dispositivo (Câmera, Firewall, Roteador, Servidor, Switch ou Sem fio). |

Preferências locais

Tabela 8.18. Formulário de preferências locais

| Campo | Descrição |
|---------------------------------------|--|
| Tamanho da página em PDF | Tamanho da página nos relatórios em PDF. |
| Limitador de pesquisa | Preencha com um valor positivo inteiro para limitar suas pesquisas. O valor padrão é 2500. |
| Primeiro período do horário comercial | Defina os horários inicial e final para o primeiro período do horário comercial. |
| Segundo período do horário comercial | Defina os horários inicial e final para o segundo período do horário comercial. |

Projeção

Configuração de padrão de parâmetros para projeção. Vá à seção projeção para dicas em como configurar estes parâmetros.

Redirecionamento de login

Preencha o campo **página de destino após login** para ser redirecionado a outro sistema após o login. No sistema redirecionado, você será capaz de acessar todos os objetos sem autenticação do TRAFip/SLAview.

Redundância

Esta seção é utilizada para especificar as configurações de redundância.

Tabela 8.19. Configurações de redundância

| Campo | Descrição |
|-----------------------------|--|
| Habilitar redundância | Escolha Sim. |
| Versão do IP | Escolha se é IPv4 ou IPv6. |
| IP de sincronização local | Preencha com o endereço de IP configurado para a interface diretamente conectada a outro appliance. |
| IP de sincronização remota | Preencha com o endereço de IP configurado para o appliance remoto. |
| Tamanho máximo de histórico | Configure o tamanho máximo de histórico em MB. O tamanho de histórico mínimo é de 16MB. |
| Interfaces | Selecione a interface que irá compartilhar os endereços de IP entre os dois appliances. Use a tecla CTRL para selecionar múltiplas interfaces. Pelo menos uma interface deve ser reservada para possuir um endereço de IP exclusivo para fins de gerenciamento. Uma interface deve ser usada para a conexão back-to-back e outras podem ser usadas para compartilhar IPs. |
| Estado preferencial | Selecione Mestre ou Slave . |

Vá à seção redundância para detalhes de habilitação deste recurso.

Registros de acesso de usuários

O sistema oferece uma ferramenta que disponibiliza um relatório sumarizado diário contendo registro de acesso de usuários. Para mais informações a respeito disso, consulte a seção **Registro de acesso**.

Você pode configurar o tempo máximo em que esses registros ficarão no sistema.

Tabela 8.20. Formulário de registros de acesso de usuários

| Campo | Descrição |
|--|--|
| Período máximo de armazenamento dos registros de acessos de usuários (meses) | Escolha um valor menor ou igual a 36. O valor padrão é 12 , ou seja, o equivalente a 1 ano. |

Relatórios

Essa seção permite fazer configurações avançadas dos relatórios.

Dados brutos do TRAFip

Preencha esses campos para configurar o formulário do relatório de dados brutos. Para mais informações a respeito desse relatório, acesse a seção Relatório de dados brutos.

Tabela 8.21. Dados brutos do TRAFip

| Campo | Descrição |
|---|---|
| Período máximo de dados por relatório (horas) | Entre com um inteiro. O padrão é 18 e o máximo valor permitido é 24 . |
| Número máximo de linhas por relatório | Entre com um inteiro. |
| Tornar padrão o tratamento de sampling rate pela configuração | Selecione Sim para preencher o campo Tratamento de sampling rate com Configuração automaticamente. |

Dados Sumarizados

Configure o período máximo de dados que um relatório pode conter. O valor padrão é **180** e o máximo valor possível é **360**.

Relatórios agendados

Configure as características que os relatórios agendados possuirão.

Tabela 8.22. Formulário de configuração dos relatórios agendados

| Campo | Descrição |
|---|---|
| Tempo de atualização da página de espera (segundos) | Entre com um inteiro. |
| Tempo Máximo de Execução (minutos) | Entre com um inteiro. |
| Número Máximo de Processos Simultâneos | Entre com um inteiro. |
| Prefixo do assunto do e-mail | Defina um prefixo para o assunto do e-mail. |
| Hostname para link do email | Configure um hostname para o e-mail. |

Servidor SMS

Método SMPP(Protocolo Short message peer-to-peer)

Use este método se o seu operador móvel disponibilizar uma conta SMPP.

Tabela 8.23. Formulário de servidor SMPP

| Campo | Descrição |
|---------------|----------------------|
| Protocolo SMS | Escolha a opção SMPP |

| Campo | Descrição |
|------------------------------|--|
| Host | Host SMPP. |
| Porta | Porta SMPP. |
| Sistema ID | Sistema ID SMPP. |
| Tipo de sistema | Tipo de sistema SMPP. |
| Senha | Senha SMPP. |
| URL | Veja a seção de URL. |
| Número de telefone de origem | Número de telefone que será mostrado como chamada SMS. |

SMSs podem ser enviadas utilizando métodos distintos. Ambos podem ser configurados por este formulário.

Método URL(Uniform Resource Locator)

Este método deve ser usado se você tiver um gateway http.

SLAview irá executar uma operação http GET utilizando a URL fornecida.

Você deve usar as wildcars \$CELLPHONE\$ e \$MSG\$ na URL.

A wildcard \$CELPHONE\$ será substituída pelo campo wildcard SMS que você preencheu no formulário de configuração do usuário.

A wildcard \$MSG\$ será substituída por uma mensagem de alarme, que contém as seguintes informações:

- Nome do alarme.
- Nível de urgência do alarme.
- Estado do alarme.
- Data e horário que o alarme mudou de estado.
- Variável de alarme.

SMTP

Preencha este formulário com os parâmetros SMTP para enviar emails.

Tabela 8.24. Formulário de parâmetros SMTP

| Campo | Descrição |
|----------------|---|
| Servidor SMTP | Configure o servidor SMTP. A porta usada pelo servidor SMTP pode ser alterada neste campo. Siga o exemplo: smtp.server.com:port |
| Usuário SMTP | Entre com o email. |
| Senha SMTP | Entre com a senha. Se o servidor SMTP não solicitar autenticação este campo pode ser deixado em branco. |
| Remetente SMTP | Configura um remetente para o email. |

Você pode verificar as configurações SMTP antes de salvar: clique em **Teste SMTP** e entre com o endereço de email para o teste.

SNMP

Coletor SNMP

Estes parâmetros serão usados para todos os processos que executam SNMP polling. Estas são configurações padrões, mas elas podem ser ajustadas a nível do dispositivo.

Para uma referência de todos os processos do sistema, vá para seção arquivos de log.

Parâmetros SNMP

| | |
|---------------------------------|---|
| SNMP Timeout | Tempo limite em segundos que a coletora irá esperar por um pacote de resposta SNMP. Intervalo de valores: 1-10. |
| Novas tentativas SNMP | Número de tentativas que serão permitidas ao dispositivo se ele não responder a uma consulta SNMP. Intervalo de valores: 1-10. |
| Número de OIDs por pacote | Número de OIDs que a coletora irá enviar em cada pacote SNMP. Intervalo de valores: 1-100. |
| Taxa máxima de envio por pacote | Número máximo de pacotes por segundo que um coletor SNMP irá enviar para cada dispositivo. |
| Janela SNMP | Número de pacotes SNMP que serão enviados sem resposta do dispositivo que está sendo sondado. |
| Porta SNMP | Porta TCP padrão para conectar com o agente SNMP. |
| Habilitar a coleta por SNMP | Habilitar a coleta SNMP para o TRAFip. Marque esta opção para habilitar o processo InterfaceCollect para pesquisar o contador de tráfego de interfaces. |
| Ignorar interfaces | Preencha a expressão para ignorar estas interfaces. |
| Interfaces high counter | Preencha a expressão para usar, nestas interfaces, o contador de OID mais alto(ifHCInOctets e ifHCOutOctets). |
| Interfaces SecRate | Preencha a expressão para usar a sec rate OIDs (IfHCIn1SecRate and IfHCOut1SecRate) nestas interfaces. |

Trap SNMP

Preencha os campos abaixo para especificar os hosts que irão receber os traps. Estes traps podem ser alarmes de ALARMmanager ou traps auto gerados pelas TELCOMANAGER MIBS.

Tabela 8.25. Campos de TRAP

| Campo | Descrição |
|-------------------------|---|
| Hosts para enviar Traps | Endereços de IP dos hosts. Ex: 10.0.0.1,10.0.0.2. |

| Campo | Descrição |
|------------------------------|-------------------------------------|
| Comunidade para enviar Traps | Comunidades SNMP dos hosts de trap. |

TACACS

Habilita o método de autenticação TACACS+. Até dois servidores podem ser configurados para Redundância.

O nome de usuário e senha para cada usuário deve ser configurado no sistema, exatamente como o servidor TACACS.

Quando este método está ativado, não existe autenticação local, ou seja, qualquer usuário que não seja do tipo **Administrador** loga pelo TACACS.

Importante

O usuário **Administrador** tem a opção de escolher logar localmente ou não, entretanto, recomenda-se que haja sempre uma conta de **Administrador** com **Autenticação local** ativada, caso seja utilizado controle de acesso externo.

Tema

Nesta seção, você pode ver o tema padrão do sistema.

Tabela 8.26. Configuração do tema

| Campo | Descrição |
|-------------|---|
| Tema padrão | Escolha o tema padrão para o sistema: Dark, Green & Yellow ou Telcomanager. |

Dica

Perceba que cada usuário pode definir seu próprio tema em configuração de usuário.

TRAFip

Ative ou desative a detecção automática de interfaces RFI (Repeated flow interface). Para ter mais informações sobre as RFI's, acesse a seção Interfaces RFI.

Transferência de arquivos

Estes parâmetros são usados para configurar os arquivos transferidos, usando o protocolo FTP, contendo objetos selecionados estaticamente por 15 minutos.

Formulário de transferência de arquivos

| | |
|--------------------------------|--|
| Endereço de IP do servidor FTP | Endereço de IP do servidor FTP. |
| Porta | Porta TCP para conectar ao servidor FTP. |
| Usuário do servidor | Nome de usuário usado para conectar ao servidor FTP. |
| Senha de usuário | Senha usada para conectar ao servidor FTP. |

Verificação de exportadores de fluxo

Com este recurso habilitado, todos os exportadores de fluxo serão checados de tempo em tempo, e para cada exportador tem um tempo sem exportação de fluxos seu ícone irá mudar, mostrando aos usuários a falta de fluxos recebidos pelo exportador.

Formulário de verificação de exportadores de fluxo

| | |
|--|--|
| Habilitar verificação de exportadores | Escolha Sim ou Não. |
| Tempo de inatividade na exportação (min) | Escolha o limite, em minutos, para cada exportador |

Verificação de versão do sistema

Todo dia entre 2h e 3h da manhã, ocorre uma verificação de versão do sistema para checar se há uma nova build disponível. Uma vez que exista, o usuário será informado.

Web Services

API de Configurações

Tabela 8.27. Formulário de API de configurações

| Campo | Descrição |
|---|---|
| Hosts com acesso permitido à API de configurações | Configure os hosts que são habilitados para acessar a API de configurações. |
| Nome de usuário utilizado pela API de configurações | Digite o usuário. |

Dados brutos do TRAFip

Configure o acesso aos dados brutos do TRAFip.

Tabela 8.28. TRAFip's raw data form

| Campo | Descrição |
|----------------------------|-----------------|
| IP com permissão de acesso | Digite o IP. |
| Senha | Digite a senha. |

Usuários

O sistema possui três tipos de usuários:

Tipos de usuário

| | |
|---------------|--|
| Administrador | Tem total acesso ao sistema. |
| Configurador | Pode criar, remover e editar qualquer objeto do sistema. Não pode fazer mudanças nas configurações do sistema. |

Operador Pode apenas visualizar o sistema de objetos monitorados e relatórios.

Quando você associa grupos a usuários, você irá restringir a visualização desse usuário a objeto com hierarquia de grupos.

Usuários também podem ser limitados aos menus que eles irão acessar e ao número de usuários simultâneos que irão acessar o sistema.

Editando usuários

1. Selecione **Sistema** → **Usuários** → **Lista de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.29. Formulário de usuário

| Campo | Descrição |
|-----------------------|--|
| Nome de usuário | Login de usuário. |
| Nome | Nome de usuário. |
| Senha | Senha. |
| Confirmação de senha | Repita a senha. |
| E-mail | E-mail para enviar alarmes e quando um relatório agendado estiver disponível. Você deve configurar o servidor SMTP. |
| SMS | Número de celular para enviar alarmes usando o protocolo SMPP ou celular@teste.com para enviar pequenos emails com alarmes. O sistema também pode enviar SMSs através da integração com um portal web. |
| Habilitar favoritos | Habilita o recurso Favoritos. |
| Usar gráfico compacto | Compacte os gráficos para que caibam na mesma página ou visualize-os no tamanho normal. |
| Autenticação local | Habilita autenticação baseada no Active Directory ou TACACS. Para configurar o Active Directory acesse Sistema → Parâmetros → Active Directory e para configurar o TACACS acesse Sistema → Parâmetros → TACACS . |
| Tema | Selecione o tema do usuário. Escolha o Tema Padrão em Sistema → Parâmetros → Tema |
| Grupo de usuário | Associa este usuário a um usuário de grupo de forma a restringir o número de acessos simultâneos ao sistema com o grupo. |
| Idioma | Selecione o idioma do usuário. |
| Perfil | Selecione o perfil de usuário para restringir o alarme e serviço de visualização de alarme e notificação. |
| Tipo | Tipo de usuário. |

| Campo | Descrição |
|--------------|--|
| Menu | Use a opção padrão para restringir o usuário a menus específicos. |
| Grupos | Selecione o grupo de subredes que o usuário será capaz de acessar. |
| Subredes | Selecione as subredes que o usuário será capaz de acessar. |

Grupos de usuários

Os grupos de usuários são usados para gerenciar quantos usuários podem estar logados simultaneamente ao sistema.

Procedimento 8.1. Gerenciando grupos de usuários

1. Selecione **Sistema** → **Usuários** → **Grupos de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.30. Formulário de usuário

| Campo | Descrição |
|---|--|
| Nome | Nome do grupo de usuários. |
| Descrição | Descrição do grupo de usuário. |
| Limitar o número de acessos simultâneos | Selecione um número entre 1 e 255. Este será o limite de acessos simultâneos no sistema com os usuários deste grupo. |
| Usuários | Especifica os usuários que irão ser colocados no grupo. Um usuário pode pertencer apenas a um grupo. |

Perfis de usuários

Os perfis de usuários são usados para associar alarmes aos usuários.

Procedimento 8.2. Gerenciando perfis de usuários

1. Selecione **Sistema** → **Usuários** → **Perfis de usuários** .
2. Clique nos botões Novo ou Editar e preencha o formulário abaixo:

Tabela 8.31. Formulário de usuário

| Campo | Descrição |
|-----------------------|---|
| Nome | Nome do perfil de usuário. |
| Token do bot Telegram | Token obtido após criar um bot no Telegram. |
| ID do chat Telegram | ID do chat no qual o bot está participando. |
| Usuários | Associa os usuários a um perfil. |

| Campo | Descrição |
|--------------------|--|
| Perfis -> Alarmes | Associa um par de Perfil -> Alarme para este perfil. |
| Alarmes de serviço | Associa serviços de alarmes a este perfil. |

Alarme Console

Você pode selecionar as colunas que serão mostradas no ALARMmanager console. Além disso, você é habilitado a configurar a ordem em que as colunas aparecerão. Para isso, basta clicar e arrastar as linhas.

Tabela 8.32. Colunas ALARMmanager console

| Coluna | Descrição |
|---------------|---|
| INÍCIO | Tempo da primeira ocorrência. |
| TÉRMINO | Tempo da última ocorrência. Mostra ATIVO se o alarme não terminou. |
| USUÁRIO | Usuário que programou o alarme. |
| TIPO | Tipo de objeto, pode ser dispositivo ou objeto mapeado. |
| OBJETO | Nome do objeto. |
| DESCRIÇÃO | Descrição do objeto. |
| IFALIAS | Se o objeto for uma interface, mostra sua ifAlias. |
| ESTADO | Estado do alarme, pode ser ativado ou desativado. |
| ALARME | Nome do alarme. |
| NÍVEL | O nível para o alarme definido em configuração de nível. |
| TRAP | Sim se foi gerado por um trap e não qualquer outro caso. |
| COMENTÁRIOS | Comentários do operador. Para inserir um comentário, clique duas vezes na célula. |

Diagnósticos

Informações de rede

Mostra a data e a hora do sistema, interfaces de rede e gateway padrão.

Testes de conectividade

Testes como ping, nslookup e traceroute para testar a conectividade entre o appliance e os elementos de rede.

Captura de pacotes

Usando essa ferramenta, você pode analisar os pacotes que estão passando pelas interfaces do appliance.

Clique em **Sistema** → **Diagnósticos** → **Captura de pacotes** .

Clique em Novo.

Tabela 8.33. Captura de pacotes

| Coluna | Descrição |
|------------------------------|---|
| Interface de rede | Escolha a interface a ser analisada. |
| Tamanho máximo do arquivo | Escolha o tamanho máximo do arquivo onde o resultado da análise será registrado. |
| Quantidade máxima de pacotes | Preencha o número máximo de pacotes a serem analisados. Preencha 0 se quiser que não tenha limites. |
| Porta | Filtra portas para analisar. Digite * para todas as portas ou vírgula para valores separados. |
| Excluir porta | Exclui portas para analisar. Digite * para todas as portas ou vírgula para valores separados. |
| Host | Escolha um host para filtrar ou selecione Todos para todos os hosts. |

Clique Enviar para iniciar a captura e depois Voltar para voltar à lista de arquivos de captura.

Se você desejar encerrar a captura, clique Parar. Um botão de Download irá aparecer e você pode fazer o download do arquivo capturado.

Objetos

Mostra o número de objetos e perfis configurados.

Estatísticas de fluxo

Mostra o máximo e a média estatística de fluxo por um período de 30 minutos, 2 horas e 24 horas.

Configure o máximo de estatística de período de armazenamento de fluxo em **Sistema** → **Parâmetros** → **Histórico de configuração** .

Sumarizador

Esta seção mostra o tempo que o processo sumarizador leva para rodar pelo último dia.

Ao implantar o sistema em arquitetura distribuída, o tempo para enviar os arquivos sumarizados de todos os coletores também será mostrado.

Importante

O processo de sumarização roda a cada cinco minutos, logo o tempo do processo rodar deve ser menor que cinco minutos para uma boa performance do sistema.

Uso de disco

Mostra informação sobre o uso de armazenamento das áreas.

| | |
|----------------------------|---|
| Logs do sistema | Logs do sistema operacional. |
| Logs SLAview | Logs do SLAview. |
| Logs TRAFip | Logs TRAFip. |
| SLAview Banco de dados TDB | Uso de armazenamento para o banco de dados SLAview Telco, que é usado para segurar os dados sumarizados do SLAview. |
| TRAFip Banco de dados TDB | Uso de armazenamento para o banco de dados TRAFip Telco, que é usado para segurar os dados sumarizados do TRAFip. |
| TRAFip dados brutos | Armazenamento usado para os dados brutos do TRAFip. |
| SLAview dados brutos | Armazenamento usado para os dados brutos do SLAview. |
| Detalhe dos dados brutos | Armazenamento dos dados brutos por dia para o sistema que você está logado. |

Arquivos de Log

Nesta área você pode visualizar os arquivos de log do sistema. Abaixo, uma lista de arquivos.

Arquivos de LOG

| | |
|--------------------|--|
| createMark.log | Logs do processo de update da versão. |
| backupgen.log | Configuração de backup diário de processos de logs. |
| dbackupArchive.log | Logs de processo remoto de backup. |
| summarizer.log | Logs do processo sumarizador. Este processo chama o processo TRAFIPsum, que processa os dados brutos do TRAFip. Quando o sistema está em arquitetura distribuída, o sumarizador é responsável por enviar arquivos sumlog (arquivos contendo dados sumarizados) para a máquina central. |
| TRAFIPsum.log | Logs do processo TRAFIPsum, que é responsável pelo processamento de dados brutos do TRAFip de acordo com as configurações. Este processo roda a cada 5 minutos. Na arquitetura distribuída, o TRAFIPsum roda nas coletoras. |
| TRAFIPlookupd.log | Logs do processo responsável pela performance de várias traduções que são usadas pelos relatórios de dados brutos do TRAFip. Exemplos: endereço de subrede IP, DNS, Netbios e aplicações de tradução. |
| Gc* | Logs do processo do coletor de lixo. |

Logs de configuração

Esta opção disponibiliza os logs da configuração do sistema.

Estes logs são mantidos por um período definido em **Sistema** → **Parâmetros** → **Histórico de configuração** → **Período máximo de armazenamento de histórico de configuração** .

Estatística de Tráfego Suspeito

São disponibilizadas estatísticas médias acerca de tráfego suspeito com dados como bytes, pacotes, fluxos e IP Flood de origem e destino para cada domínio.

Fuso horário

Este menu é usado para configurar o fuso horário correto para o servidor. Existem 4 fusos pré-definidos: **Brasília**, **Acre**, **Fernando de Noronha** e **Amazônia**. Você pode selecionar um deles ou fazer o upload de um novo fuso.

Este procedimento é usualmente necessário se existem modificações de dados durante o dia.

Suporte

Esta opção pode ser usada para estabilizar uma conexão segura para os servidores de suporte da internet da Telcomanager.

Uma vez que a conexão é estabelecida, você pode contactar o time de suporte da Telcomanager com o código de serviço.

Dica

Se seu código de serviço não funcionar, tente entrar com um diferente código de serviço.

Sobre

Esta seção lista a versão que está atualmente instalada e as opções de licença.

Você também pode chegar o número de dispositivos existentes, a série de dados históricos e o limite bits/s ou flow/s.

Capítulo 9. ALARMmanager

Relatórios

Para acessar os relatórios ALARMmanager, vá até **ALARMmanager** → **Relatórios**

Relatórios suprimidos

Este relatório fornece os logs de todas as operações de supressão realizadas pelos usuários.

Tabela 9.1. Formulário de relatório de alarmes suprimidos

| Campo | Descrição |
|-------------------|---|
| Formato de saída | Selecione um dos formatos para o relatório: HTML, CSV ou PDF. |
| Tipo de objeto | O tipo de objeto para o alarme. |
| Instante inicial | O instante inicial para o relatório. |
| Instante final | O instante final para o relatório. |
| Operação | Filtro para operação de supressão. |
| Filtro de usuário | Filtra pelo usuário que executou a operação. |
| Filtro de objeto | Filtra pelo objeto em que a operação foi executada. |
| Filtro de alarme | Filtra pelo alarme em que a operação foi executada. |

Relatórios consolidados

Este relatório disponibiliza uma visão de todos os eventos de alarme de maneira detalhada ou resumida.

Este relatório pode ser salvo como um template. Para instruções em como trabalhar com templates de relatório, vá à seção templates neste manual.

Tabela 9.2. Formulário de alarmes consolidados

| Campo | Descrição |
|--------------------------|---|
| Filtro de alarme | Use expressão regular e clique no botão Filtrar para selecionar o alarme desejado. |
| Filtro de objeto | Use expressão regular para filtrar os objetos desejados. |
| Fabricante | Filtrar pelo fabricante do objeto. Você tem que usar expressão regular para filtrar. |
| Tipo de fabricante | Filtrar pelo tipo de fabricante. Você tem que usar expressão regular para filtrar. |
| Tipo de objeto analisado | Tipo do objeto. |
| Filtro ifAlias | Filtra baseado na interface OID ifAlias. Você deve usar expressão regular para filtrar. |
| Instante inicial | Período inicial de análise. |
| Instante final | Período final de análise. |

| Campo | Descrição |
|--------------------------|---|
| Período | Se a opção Dia todo estiver marcada, este campo é ignorado, ao contrário, o dado é selecionado com aquele intervalo para cada dia. |
| Excluir fins-de-semana | Excluir período de fins-de-semana do relatório de dados. |
| Somente ativos | Mostra apenas os alarmes ativos. |
| Consolidado | Esta opção irá sumarizar todas as ocorrências de alarme para cada objeto. |
| Somente gerados por trap | Mostra apenas alarmes gerados por traps link down . |
| Formato de saída | Selecione um dos formatos para o relatório: HTML, PDF ou CSV. |
| Grupos | Este campo pode ser usado para filtrar objetos associados a apenas alguns grupos de root. |

Dica

Para ordenar os resultados do relatório, clique em cada cabeçalho da coluna.

Template de Email

Introdução

Você pode selecionar o formato de e-mail do ALARMmanager e escolher se você deseja utilizar o template padrão ou personalizá-lo.

Tabela 9.3. Template de Email

| Campo | Descrição |
|-------------------------------------|--|
| Habilitar template de e-mail padrão | Selecione Não para customizar o template de email. |
| Conteúdo de e-mail | Você pode escolher o formato de e-mail que você irá receber (HTML ou Txt). |

Customizando o e-mail

Quando você está editando seu template de e-mail, é possível restaurar o padrão apenas clicando no padrão **Restaurar template padrão**.

Se o conteúdo de e-mail está em formato HTML, você pode ter uma pré-visualização antes de salvar o novo template. Para fazer isto, clique no botão **Preview**.

Você terá as seguintes palavras chave entre '\$' e você pode substituí-las para sua configuração de alarme:

Tabela 9.4. Variáveis de e-mail

| Variáveis | Descrição |
|------------------|--|
| \$date\$ | Data de ativação/desativação do alarme. |
| \$objtype\$ | Tipo do objeto: Objeto mapeado ou Device. Alarme de serviço não possui tipo de objeto. |

| Variáveis | Descrição |
|----------------|--|
| \$object\$ | Nome do objeto. |
| \$path\$ | Exibe o caminho para o objeto no SLAview. |
| \$alarm\$ | Nome do alarme. |
| \$action\$ | Estado do alarme: ativado ou desativado. |
| \$level\$ | Nível de urgência do alarme. |
| \$formula\$ | Fórmula do alarme. |
| \$varbind\$ | Varbind. |
| \$suppressed\$ | Indica se o alarme foi suprimido. |
| \$color\$ | Variável para ser usada no e-mail HTML. Verde para desativado e vermelho para ativado. |

Níveis de urgência de alarme

Os níveis de urgência na aplicação ALARMmanager são customizáveis e você pode configurar quantos quiser.

Para gerenciar os níveis de alarme, acesse o menu **ALARMmanager** → **Níveis de urgência de alarme**.

Aqui você possui uma lista de níveis pré-configurados. Você pode editar níveis e adicionar outros.

Mudando o nível de prioridade da urgência

Para mudar o nível de prioridade de urgência, selecione o nível desejado e clique nas setas UP ou DOWN localizadas no canto superior esquerdo.

Adicionando um novo nível de urgência

Para adicionar um nível de urgência, clique no botão Novo e preencha o formulário.

Tabela 9.5. Formulário de nível de urgência de alarme

| Campo | Descrição |
|-----------------------|--|
| Rótulo | Defina uma legenda para o nível de urgência. Ela será mostrada em uma coluna do ALARMmanager console. |
| Cor do plano de fundo | A cor do plano de fundo que será mostrada no ALARMmanager console. |
| Cor do texto | Cor do texto que será mostrado no ALARMmanager console. |
| Aviso sonoro | Habilita som de aviso para este alarme. O som de aviso irá ser tocado pelo Java ALARMmanager Console se esta função também estiver habilitada no console. Para habilitá-la, acesse ALARMmanager → Console → botão ALARMmanager → Ferramentas |

| Campo | Descrição |
|--------------------|---|
| Alarmes | Selecione os alarmes que irão receber esta prioridade. |
| Alarmes de serviço | Selecione os alarmes de serviço que irão receber esta prioridade. |

Alarmes

Os alarmes são baseados no tráfego medido de objetos configurados no sistema. Existem dois tipos de alarmes: Padrão e Histórico.

Para configurar ambos os tipos de alarme, selecione **ALARMmanager** → **Alarmes**, clique no botão **Novo** e preencha o formulário.

Você pode criar um alarme para tipo de objeto:

- Dispositivo
- Interface
- Grupo de Interface
- Subrede
- Grupo de Subrede
- Aplicações
- Grupo de Aplicação
- Protocolos
- Sistemas autônomos
- Grupo de Sistemas Autônomos
- ToS
- Grupo de ToS
- Tag

Configuração de alarmes padrão

Este tipo de alarme é usado para análise de tráfego imediata, quando não tem condições possíveis para determinar a fórmula. Use este alarme para manter controle sobre as condições de contorno que necessitam de tratamento quando detectadas.

Tabela 9.6. Formulário de alarme padrão

| Campo | Descrição |
|----------------|--|
| Nome | Texto descritivo para o alarme. Ex.: alto tráfego, sem tráfego HTTP. |
| Tipo de alarme | Escolha padrão. |
| Fórmula | Veja a seção Fórmula de alarmes padrão. |

| Campo | Descrição |
|--|---|
| Varbind | Campo de texto livre que pode ser usado para reconhecer os alarmes que são encaminhados como traps. |
| Email | Veja a seção de ações. |
| Dispositivo móvel | Veja a seção de ações. |
| Trap | Veja a seção de ações. |
| Enviar email após (minutos) | Veja a seção de ações. |
| Enviar mensagens de dispositivo móvel após (minutos) | Veja a seção de ações. |
| Enviar trap após (minutos) | Veja a seção de ações. |
| Desabilitar trap para alarme suprimido | Se a opção "Não" é selecionada, a trap será enviada e a condição de supressão será indicada nela. A opção "Sim" irá prevenir que a trap seja enviada. |
| Desabilitar mensagens de dispositivo móvel para alarme suprimido | Se a opção "Não" é selecionada, as mensagens de dispositivo móvel serão enviadas e a condição de supressão será indicada nele. A opção "Sim" irá prevenir que as mensagens de dispositivo móvel sejam enviadas. |
| Desabilitar email para alarme suprimido | Se a opção "Não" é selecionada, o email será enviado e a condição de supressão será indicada nele. A opção "Sim" irá prevenir que o email seja enviado. |
| Ocorrências consecutivas para armar | Escolha o número de ocorrências consecutivas da fórmula de alarme que deve disparar o alarme. Não utilizado em alarmes de Trap. |
| Não ocorrências consecutivas para desarmar | Escolha o número de não-ocorrências consecutivas da fórmula de alarme que deve desarmar o alarme. Não utilizado em alarmes de Trap. |
| Nível de urgência | Selecione o nível para o alarme. |
| Perfil de alarme | Selecione os perfis de alarme aos quais ele deve pertencer. |

Fórmula de alarmes padrão

TRAFip mede e divide o tráfego em três diferentes formas: bps (bits por segundo), pacotes e fluxos. Cada um desses é utilizado como uma métrica na fórmula do alarme. Essas métricas podem ser absolutas ou podem pertencer ao perfil de tráfego. Desta forma, nós podemos referenciar métricas na fórmula de alarme através da sintaxe:

1. **Absoluto:** "Nome do domínio".self.<métrica>
2. **Perfil de tráfego:** "Nome do domínio".self.<tipo de perfil>[<"nome do perfil">.<"nome do item de perfil">].<métrica>

As métricas acima mencionadas podem ser chamadas de **curvas**.

Os tipos de análises de perfil podem ser Matriz, Distribuição e Conteúdo, representados por **MTX**, **DST** e **CNT**, respectivamente.

As métricas podem ser representadas de acordo com a seguinte tabela:

Tabela 9.7. Representação das métricas

| Métrica | Sintaxe |
|-------------------------|-----------------------------------|
| Bps (bits/s) de origem | bytAb |
| Bps (bits/s) de destino | bytBa |
| Pacotes de origem | pktAb |
| Pacotes de destino | pktBa |
| Fluxo de origem | flwAb |
| Fluxo de destino | flwBa |
| Limite do objeto | limit (Veja a nota abaixo) |

Importante

A métrica **limit** refere-se ao limite do objeto associado ao alarme e, caso não haja limite (dispositivo), o mesmo será ignorado. Ao utilizar esta métrica, você não precisará especificar o domínio. Veja o exemplo a seguir: `(self.limit) > 0`

Você deve construir a fórmula utilizando as seguintes regras:

- Use parênteses "(" para precedência da operação.
- Use os operadores lógicos AND e OR.
- Use os operadores de comparação ==, !=, <, >, <=, >=.
- Use os símbolos *, -, + e / para executar as operações.

Veja os exemplos abaixo:

1. **Absoluto:** `("Default".self.bytab) > 0`
2. **Perfil de tráfego:** `("Default".self.CNT["Applications"."ssh"].bytab) > 0`

Configuração do alarme de mudança de comportamento

Este tipo de alarme é usualmente configurado para quando você não pode definir os limites de forma explícita, mas ainda quer ser avisado de mudanças no comportamento típico dos objetos.

Tipicamente, este tipo de alarme é usado por objetos que podem mostrar evolução gradual sobre o tempo (um aumento da largura de banda, por exemplo). Nestes casos, definir limites estáticos podem levar a disparos de alarmes desnecessários. Para resolver isto, você pode configurar o sistema para definir, em uma base diária, um comportamento linear padrão para o objeto que você deseja monitorar - esta linha representa o comportamento futuro esperado do objeto.

O alarme será disparado comparando o esperado e a métrica coletada, levando em consideração uma tolerância definida pelo usuário. O valor esperado para curva configurada no alarme é calculado considerando um período de tempo definido por você.

Tabela 9.8. Formulário de alarme histórico

| Campo | Descrição |
|-------|---|
| Nome | Texto descritivo para o alarme. Ex.: alto tráfego, nenhum tráfego HTTP. |

| Campo | Descrição |
|--|--|
| Tipo de alarme | Escolha Histórico . |
| Varbind | Um campo de texto livre que pode ser usado para reconhecer os alarmes que são encaminhados como trap. |
| Horário de ativação | Veja a seção ativação de fórmulas de alarme. |
| Curva | Veja a seção mudança do comportamento da curva de alarme. |
| Histórico mínimo (dias) | Mínima quantidade de dias necessários para preencher o período de análise. |
| Histórico máximo (dias) | Máxima quantidade de dias permitida para preencher o período de análise. |
| Número de violações consecutivas (dias) | Veja a seção Número de violações consecutivas. |
| Fator de tolerância | Este fator é medido com desvio padrão e é usado para comparar valores esperados com o valor atual. Veja a seção Fator de tolerância. |
| Período de alarme (minutos) | Veja a seção Período de alarme. |
| Email | Veja a seção de ações. |
| Dispositivo móvel | Veja a seção de ações. |
| Trap | Veja a seção de ações. |
| Enviar email após (minutos) | Veja a seção de ações. |
| Enviar mensagens de dispositivo móvel após (minutos) | Veja a seção de ações. |
| Enviar trap após (minutos) | Veja a seção de ações. |
| Desabilitar trap para alarme suprimido | Se a opção não é selecionada, o trap será enviado e a condição de supressão será indicada na trap. A opção sim irá prevenir que a trap seja enviada. |
| Desabilitar sms para alarme suprimido | Se a condição não é selecionada, o sms será enviado e a condição de supressão será indicada no sms. A opção sim irá prevenir que o sms seja enviado. |
| Desabilitar e-mail para alarme suprimido | Se a opção não é selecionada, o e-mail será enviado e a condição de supressão será indicada no e-mail. A opção sim irá prevenir que o e-mail seja enviado. |
| Ocorrências consecutivas para armar | Escolha o número de ocorrências consecutivas da fórmula de alarme que deve disparar o alarme. |
| Não ocorrências consecutivas para desarmar | Escolha o número de não-ocorrências consecutivas da fórmula de alarme que deve desarmar o alarme. |
| Nível de urgência | Selecione o nível para o alarme. |
| Perfil de alarme | Selecione os perfis de alarme aos quais ele deve pertencer. |

Fórmula de alarmes históricos

Este campo é utilizado apenas para alarmes históricos. Ele define quando uma ocorrência de alarme deve ser gerada.

As variáveis usadas são **weekday** e **time**. As duas outras variáveis utilizadas são: **everyday**, para disparar o alarme todo dia da semana e **everytime**, para disparar o alarme todo tempo do dia.

Se você deseja definir quando um alarme deve ser gerado, você pode usar as variáveis weekday e time com os operadores definidos. Os valores para weekday devem ser entre 1 (domingo) e 7 (sábado). Para a variável time, você deve usar HH:MM.

Exemplo:

```
weekday > 1 and weekday < 7
```

Esse alarme disparará se o dia da semana estiver entre domingo e sábado.

Curvas de alarmes históricos

O TRAFip mede e divide o tráfego em três diferentes formas: bps (bits/segundo), pacotes e fluxos. Cada um deles é usado como métrica na curva do alarme de mudança de comportamento. Essas métricas podem ser absolutas ou podem pertencer a um perfil de tráfego. Desta forma, podemos referenciar a métrica da curva de um alarme de mudança de comportamento através da seguinte sintaxe:

1. **Absoluta:** "Nome do Domínio".self.<métrica>
2. **Perfil de tráfego:** "Nome do Domínio".self.<tipo de perfil>[<nome do perfil>.<nome do item de perfil>].<métrica>

Tipos de perfil podem ser Matriz, Distribuição e Conteúdo, representados por **MTX**, **DST** e **CNT**, respectivamente.

Métricas podem ser representadas de acordo com a seguinte tabela:

Tabela 9.9. Representação de métricas

| Métrica | Sintaxe |
|-------------------------|--------------|
| Bps (bits/s) de origem | bytAb |
| Bps (bits/s) de destino | bytBa |
| Pacotes de origem | pktAb |
| Pacotes de destino | pktBa |
| Fluxos de origem | flwAb |
| Fluxos de destino | flwBa |

Número de violações consecutivas

A violação das amostras será considerada se elas acontecerem consecutivamente e o número de violações for acima do parâmetro especificado, ao contrário elas serão descartadas da computação do comportamento.

Por exemplo, suponha que você tenha uma mudança de comportamento no alarme para um tráfego de interface e que, em algum momento, o tráfego era 500MB +- 300MB e o tráfego detectado era 3GB. Esta amostra não será usada na computação comportamental e o tráfego esperado para o dia seguinte continuará

sendo 500MB. Esta amostra será apenas utilizada se tiverem N amostras consecutivas violadas, o que caracteriza um novo comportamento.

Fator de tolerância

O TRAFip irá executar o seguinte cálculo para determinar se o valor observado representa uma mudança de comportamento:

```
IF (AV < (EV - (N * SD)) OR AV > (EV + (N * SD)))  
Em seguida aciona o comportamento da mudança do alarme.
```

Onde

N é o fator de tolerância

SD é o desvio padrão da curva

AV é o valor médio para a atual meia-hora

EV é o valor médio esperado para a atual meia-hora

Período de alarme

O TRAFip irá mostrar a amostra a cada 30 minutos ou a cada 5 minutos.

Quando um período de alarme é configurado como 5 minutos, o sistema irá mostrar a média do valor para cada 5 minutos e comparará com o valor esperado, mas não salvará se for uma mudança de comportamento.

Quando um período de alarme é configurado como 30 minutos, o sistema irá mostrar o valor da média para cada meia hora e determinará se o valor representa uma mudança de comportamento.

Ações

A cada momento o sistema do TRAFip processa um tráfego de 5 minutos, todas as fórmulas de alarme são avaliadas e se retornarem verdadeiro, a ocorrência é gerada. O alarme irá disparar para uma ocorrência de alarme apenas se o número de ocorrências consecutivas for ultrapassado.

Quando você marca uma ação para um alarme, você tem que preencher três campos:

Campo de ações

| | |
|--|--|
| Ocorrências consecutivas para armar | Isto representa o número de vezes consecutivas em que o limite é ultrapassado. |
| Não ocorrências consecutivas para desarmar | Isto representa o número de vezes consecutivas em que o limite não é ultrapassado. |
| Nível de urgência | Escolha um nível de urgência adequado para o alarme. |

Tipos de ações

| | |
|-------|---|
| Email | Um email será enviado aos usuários. O servidor SMTP do TRAFip deve ser configurado, bem como o email de cada usuário no formulário de configuração do usuário. O email será enviado depois do número de segundos definido no campo Enviar email após (minutos) , começando do tempo de ativação. |
|-------|---|

| | |
|-----------------------------|---|
| Dispositivo móvel(SMS) | Mensagens mais curtas que as enviadas por email. Este alarme pode ser enviado para um email pelo gateway de SMS se o campo de SMS estiver configurado no seguinte formato: 88888888@operador.com. Se o SMS é um número de telefone, os protocolos SMPP ou HTTP também podem ser usados para enviar a mensagem. Para fazer isto, você precisa configurar o seguinte item: Sistema → Parâmetros → Servidor SMS . |
| Dispositivo móvel(Telegram) | Uma mensagem será enviada para um chat do Telegram por um bot. Para configurar esta funcionalidade , você deve criar um bot no Telegram, para fazê-lo, uma vez no Telegram, inicie uma conversa com o usuário @BotFather. Escolha a opção /newbot e siga as instruções para finalizar a criação do bot. Ao terminar anote o token do bot Telegram. Associe o bot ao chat no qual as mensagens serão enviadas. Acesse o formulário de perfil de usuários, preencha o campo "Token do bot Telegram" e clique em Validar. Se tudo correr bem, o campo "ID do chat Telegram" será automaticamente preenchido. A mensagem será enviada após os segundos definidos no campo Enviar mensagem após , iniciando pelo tempo de ativação do alarme. |
| Trap | Uma trap será enviada para cada alarme. A trap deve ser interpretada usando a MIB TELCOMANAGER-ALARMMANAGER-MIB.my, que está disponível na lista de MIB do SLAview. Você também deve configurar o servidor para enviar as traps em Sistema → Parâmetros → SNMP → SNMP trap . A trap será enviada depois do número de segundos definidos no campo Enviar trap após (minutos) , começando do tempo de ativação. |

Gerenciamento de supressão de alarmes

Nesta seção você irá aprender como gerenciar todas as tuplas de alarme/objeto as quais o usuário possui acesso.

Para suprimir, siga o procedimento abaixo:

1. Vá para guia **ALARMmanager** → **Alarmes** e clique no botão Alarmes suprimidos.
2. Preencha os campos do filtro desta forma para selecionar os alarmes/objetos desejados e clique no botão Filtro.
3. Selecione os alarmes/objetos da lista.
4. Preencha o campo razão de supressão se desejado.
5. Clique no botão Salvar para suprimir os alarmes/objetos selecionados.

Para tirar a supressão dos alarmes, siga o mesmo procedimento, mas deselegione os alarmes/objetos desejados.

Importante

Perceba que se o alarme já está suprimido, ele não será suprimido novamente e o mesmo acontece à ação de desuprimir.

Importante

Alarmes suprimidos podem ser considerados para colorir o mapa usando a flag "Considerar suprimido" no MapView. Se um alarme suprimido é inativado por um momento e depois fica ativo, ele é marcado como suprimido.

Configuração de perfil de alarme

Perfis são usados para juntar os alarmes e os objetos monitorados.

Para configurar um perfil de alarme, selecione **ALARMmanager** → **Perfil de alarme**, clique no botão **Novo** e preencha o formulário.

Tabela 9.10. Formulário de perfil de alarme

| Campo | Descrição |
|----------------------------|--|
| Nome | Texto descritivo para um perfil de alarme. |
| Alarme | Selecione os alarmes desejados para este perfil. |
| Caixa de seleção de objeto | Primeiramente, selecione o tipo de objeto e os objetos disponíveis serão mostrados. Depois, selecione os objetos desejados para este perfil. |

Alarmes de serviço

Introdução

O recurso de alarmes de serviço permite que você junte alarme de diferentes objetos em uma única fórmula. Agora o TRAFip pode disparar o alarme sob condições mais sofisticadas.

Você será capaz de criar, por exemplo, os seguintes alarmes:

- Um alarme que é ativo quando um link de WAN tem uma alta latência e também possui um baixo tráfego.
- Um alarme para lhe dizer quando ambos o primário e os links de backup de locação irão falhar.

Fórmula

Nas fórmulas você pode usar os operadores lógicos OR, AND, NOT e XOR para construir fórmulas mais complexas.

Console

Introdução

A aplicação ALARMmanager trabalha de forma integrada entre os sistemas e é capaz de gerar alarmes baseados em fórmulas.

Ela também possui os seguintes recursos:

- Interface gráfica em HTML5.

- Alarme através de email, mensagens de dispositivo móvel e traps.
- Interface gráfica para criar alarmes e fórmulas customizadas.
- Alarmes podem emitir sons.
- Perfis de alarme para facilitar a associação de alarmes aos objetos gerenciados.
- Reconhecimento de alarmes e comentários.
- Supressão de alarmes para evitar emails, mensagens de dispositivo móvel e traps para alarmes repetidos.

Operação de Console

Para acessar o console operacional de alarme, vá em **ALARMmanager** → **Console**

Autenticação

Um usuário deve estar autenticado para acessar o ALARMmanager.

Console

O console do ALARMmanager irá mostrar todos os alarmes que estão ativos e também inativos que ainda não foram inativos pelo parâmetro de período de armazenamento do ALARMmanager. Os alarmes que você poderá visualizar dependerão da permissão que o seu usuário possui.

Você pode configurar as colunas em **Sistema** → **Usuários** → **Alarm console** .

O console possui as seguintes colunas:

Tabela 9.11. ALARMmanager console

| Coluna | Descrição |
|-------------|---|
| INÍCIO | O momento da primeira ocorrência. |
| TÉRMINO | O momento da última ocorrência. Mostra ATIVO se o alarme ainda não terminou. |
| USUÁRIO | Usuário que programou o alarme. |
| TIPO | Tipo de objeto, pode ser dispositivo ou objeto mapeado. |
| OBJETO | Nome do objeto. |
| DESCRIÇÃO | Se o objeto é uma interface, mostra seu ifAlias. |
| CAMINHO | Mostra o primeiro caminho para o objeto nos grupos SLAview. |
| ESTADO | Estado do alarme, pode ser ativo ou inativo. |
| ALARME | Nome do alarme. |
| NÍVEL | O nível do alarme definido na configuração de nível. |
| TRAP | Sim se foi gerado por um trap e não caso contrário. |
| COMENTÁRIOS | Comentário pelo operador. Para inserir um comentário, clique duas vezes naquela célula. |

Reconhecimento de alarme

Uma vez que o alarme é reconhecido, a linha de alarme mostra o nome de usuário que executou a operação e sua informação também pode ser vista em relatórios de alarmes consolidados. Depois de reconhecer um alarme, você é capaz de inserir comentários para o alarme.

Para reconhecimento de alarme, clique com o botão direito nele e depois selecione a opção Reconhecer alarmes no menu. O alarme é depois mostrado na tabela de alarmes reconhecidos para todos os operadores.

Para múltiplos reconhecimentos de uma vez, selecione com o botão esquerdo do mouse e depois clique com o botão direito na lista para mostrar o menu.

O alarme pode ser liberado do operador apenas pelo usuário administrador. Para isso, o administrador deve selecionar o alarme de reconhecimento na lista e selecionar a opção de alarme Liberar alarmes no menu.

Supressão de alarme

O mecanismo de supressão de alarme permite que você suprima qualquer tupla de alarme/objeto, desde que o alarme já esteja configurado para aquele objeto. A supressão também desabilitará e-mails, mensagens de dispositivo móvel e traps para o alarme/objeto ou indicará esta condição nos e-mails, mensagens de dispositivo móvel e traps. Você pode configurar o comportamento desejado neste campo em configuração de alarme.

Para suprimir um alarme siga o procedimento abaixo:

1. Selecione o alarme desejado com o botão esquerdo do mouse. Para escolher mais de um alarme, segure a tecla CTRL e selecione os alarmes com o botão esquerdo do mouse.
2. Clique com o botão direito do mouse para mostrar o popup menu. Clique na opção Suprimir alarmes no popup menu.
3. Preencha a caixa de texto com a razão de supressão. Você também pode deixá-la em branco.
4. Clique no botão Confirmar.

Você pode checar as operações de supressão de log executadas pelos usuários em relatório de alarmes suprimidos.

Você pode gerenciar a lista de supressão de alarme/objeto em **ALARMmanager** → **Alarmes** → **Supressão de alarmes**.

Comentário de alarmes

Para inserir comentários para um alarme, primeiramente você precisa reconhecê-lo.

Para inserir um comentário, siga o procedimento abaixo:

1. Clique na tabela "Reconhecidos".
2. Dê um duplo clique na coluna COMENTÁRIOS para o alarme.
3. Preencha a caixa de texto na janela Comentários de Alarme e clique no botão Confirmar.

Habilitar som para um alarme

O som do alarme irá funcionar se tiver um ativo, não reconhecido, Critical ou Major no ALARMmanager console.

Selecione a opção **ALARMmanager** → **Console** → **Habilitar aviso sonoro** .

Sincronização de alarme

O ALARMmanager sincroniza seus alarmes com o banco de dados do sistema a cada 2 minutos. Esta sincronização pode ser acionada imediatamente no menu **ALARMmanager** → **Console** → **Sincronizar alarmes** .

Excluindo alarmes

O ALARMmanager deleta automaticamente os alarmes que tenham terminado, mas você será capaz de visualizá-los depois no console até que o armazenamento máximo de alarmes inativos tenha passado. Para configurar este parâmetro vá ao menu **Sistema** → **Parâmetros** → **ALARMmanager** .

O operador pode deletar os alarmes a qualquer momento se ele estiver no estado inativo, selecionando os alarmes com o botão direito no mouse e clicando na opção Apagar no popup menu.

Abrir gráficos

Selecione uma linha de alarme e clique no botão Abrir gráficos para abrir os gráficos do objeto.

Filtro de alarme

Este filtro pode ser acionado de qualquer objeto em qualquer mapa. Isto irá filtrar os alarmes dos objetos e também dos objetos relacionados a ele hierarquicamente.

Capítulo 10. Recursos habilitados com licença

Redundância

A solução de redundância te habilita a implantar dois appliances idênticos trabalhando em modo HOT-STANDBY.

Importante

Essa funcionalidade só funcionará se os dois appliances estiverem na mesma versão.

Dica

É aconselhável que os appliances tenham as mesmas configurações de hardware. Caso haja diferenças, o sistema mostrará um aviso.

Conceitos

- Quando este recurso é habilitado, o sistema trabalha com duas máquinas idênticas em HOT-STANDBY realizando a sincronização dos dados e observando cada um dos estados a todo momento.
- Um protocolo de comunicação roda entre os dois servidores e, se uma falha é detectada em um dos servidores, o outro irá agir como o servidor ativo - se ele já não estiver - e a trap `tmTSRedundancyStateChangeTrap` será enviada. Esta trap é documentada na MIB `TELCOMANAGER-TELCOSYSTEM-MIB`.
- Ambos appliances compartilham o mesmo endereço IP, que é usado para enviar fluxos dos roteadores. Este endereço de IP é ativo apenas no servidor ATIVO e quando mudam de estado, o endereço MAC da interface irá migrar para o servidor ATIVO.

Habilitando a redundância

1. Usando dois appliances Telcomanager idênticos com a opção de licença de redundância habilitada, faça uma conexão back-to-back usando a mesma interface em cada dispositivo e configure um endereço de IP não-válido entre aquelas interfaces, usando CLI (command line interface) em cada dispositivo.
2. Na CLI, configure o endereço de IP que será compartilhado entre dois servidores apenas no servidor ativo.
3. Vá ao menu **Sistema** → **Parâmetros** → **Redundância** e preencha o formulário de ambos os dispositivos.
4. Espere 20 minutos para verificar o estado de cada servidor em **Sistema** → **Diagnósticos** → **Informação de rede**.

Arquitetura distribuída

Conceitos

A arquitetura distribuída deve ser usada para dimensionar a capacidade do sistema para coletar fluxos de IP e dados SNMP e para processar os dados brutos, uma vez que essas tarefas são designadas ao appliance coletor.

Pré-requisitos

- Todas as máquinas envolvidas devem ter o mesmo acesso SNMP para todos os dispositivos monitorados.
- Os fluxos de IP devem ser exportados para os appliances coletores.
- Deve possuir largura de banda suficiente para transferir os arquivos de sumarização entre os appliances coletores e appliance central. Mantenha em mente que um coletor requer em torno de 64 Kbps de largura de banda para monitorar 1000 interfaces com 10 variáveis de sumarização em cada interface.
- As portas TCP 22 e 3306 devem estar disponíveis entre o appliance coletor e o central. A porta 22 é usada para transferir arquivos no protocolo SSH e a 3306 é utilizada para emitir consulta do banco de dados para o appliance central.

Implantação

1. No appliance central, vá em **Sistema** → **Parâmetros** → **Arquitetura distribuída** e preencha o formulário.
2. No appliance coletor, vá em **Sistema** → **Parâmetros** → **Arquitetura distribuída**.
3. No appliance central, vá em **Configuração** → **Coletoras** e preencha o formulário.
4. Espere em torno de 20 minutos e vá ao menu **Configuração** → **Coletoras**, para checar se as coletoras listadas estão com o menu em status **ON**.