Automatize a largura de banda sob demanda caso de uso por meio da pilha de software de automação de loop fechado

Contents

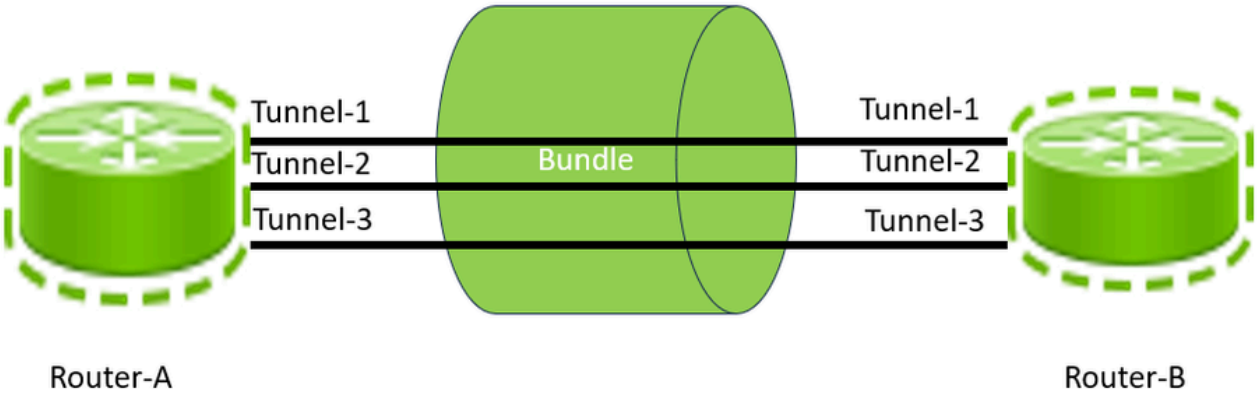
Introdução

Este documento descreve os componentes em uma solução de automação de loop fechado da Cisco para a automação de escala de túnel do Generic Routing Encapsulation (GRE) e sua adaptabilidade para outros casos.

Informações de Apoio

Os provedores de serviços querem assumir o controle de suas utilizações de largura de banda nos túneis GRE em sua rede e monitorá-los de perto para dimensionar túneis conforme necessário usando uma solução de automação de loop fechado inteligente.

O GRE é um protocolo de tunelamento que fornece uma abordagem genérica simples para transportar pacotes de um protocolo sobre outro usando o encapsulamento. Este documento enfoca o exemplo baseado em túnel GRE para a plataforma Cisco IOS® XRv, mas também pode ser generalizado para outras plataformas. O GRE encapsula um payload, um pacote interno que precisa ser entregue a uma rede de destino dentro de um pacote IP externo. O túnel GRE se comporta como um link ponto-a-ponto virtual com dois pontos finais identificados pelo endereço origem e destino do túnel.



Túneis GRE entre roteadores

Configurar um túnel GRE envolve criar uma interface de túnel e definir a origem e o destino do túnel. Esta imagem mostra a configuração de três túneis GRE entre o Roteador A e o Roteador B. Para essa configuração, é necessário criar três interfaces, cada uma no Router-A, como Tunnel-1, Tunnel-2 e Tunnel-3, e criar de forma semelhante três interfaces no Router-B, como Tunnel-1, Tunnel-2 e Tunnel-3. Entre dois roteadores provedores de serviços, pode haver vários túneis GRE. Cada túnel, assim como qualquer outra interface de rede, tem uma capacidade definida baseada na capacidade da interface. Portanto, um túnel só pode transportar um tráfego máximo igual à sua largura de banda. O número de túneis é frequentemente baseado na previsão inicial de carga de tráfego e utilização de largura de banda entre dois locais (Roteadores). Com as mudanças na expansão da rede e da rede, espera-se que essa utilização da largura de banda mude. Para otimizar o uso da largura de banda da rede, é importante adicionar novos túneis ou remover túneis extras entre dois dispositivos com base na utilização da largura de banda medida em todos os túneis entre os dois dispositivos.

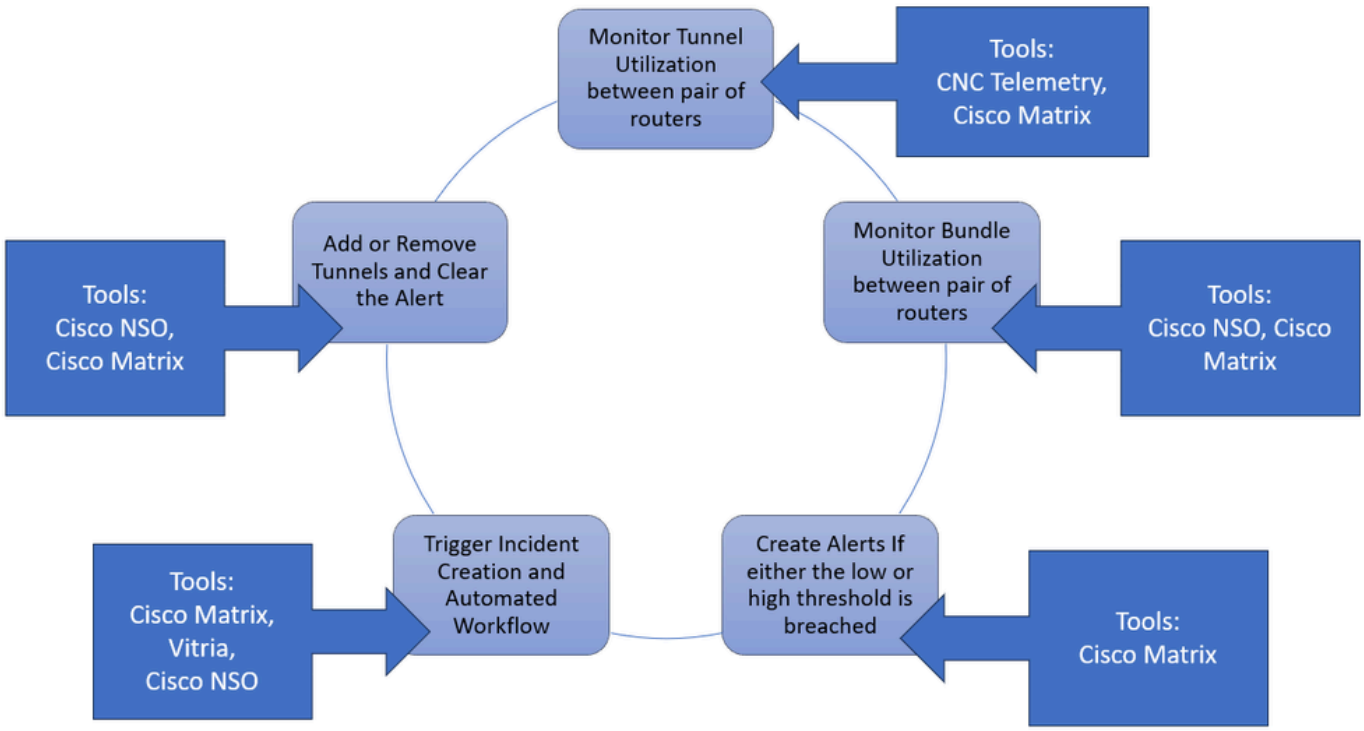
Neste exemplo, você pode dizer que a capacidade total dos três túneis entre o Roteador-A e o Roteador-B é a soma das capacidades de Tunnel-1, Tunnel-2 e Tunnel-3, que é chamada de largura de banda agregada ou largura de banda no nível do pacote GRE. Observe que a palavra-chave 'bundle' aqui se refere aos túneis entre um par de roteadores; não se pretende nenhuma relação implícita com o agrupamento de links LACP/Etherchannel. Além disso, o tráfego real entre os dois roteadores é o tráfego agregado total através de Tunnel-1, Tunnel-2 e Tunnel-3. Geralmente, você pode conceber um conceito de utilização de largura de banda no nível do pacote, que pode ser uma razão entre o tráfego total através dos túneis e a capacidade total de todos os túneis entre dois roteadores. Geralmente, qualquer provedor de serviços deseja tomar uma ação corretiva adicionando ou removendo túneis entre dois roteadores se observar que a largura de banda está sendo utilizada em excesso ou subutilizada. No entanto, para este documento, considere que o limite inferior é de 20% para baixa utilização e 80% para alta utilização para a utilização do nível de pacote entre dois roteadores.

Requisitos

1. A solução de loop fechado é necessária para executar a automação completa de loop fechado do pacote GRE no XRv9K, no qual o sistema pode coletar dados de telemetria, monitorar os dados na forma de KPIs (Key Performance Indicators, principais indicadores de desempenho), aplicar agregação, criar TCA (Threshold Cross Alerts, alertas cruzados de limite) e executar a configuração de correção automatizada, e fechar o alerta.
2. A solução pode calcular um Indicador Chave de Desempenho (KPI) de Rede para fornecer a Utilização de Largura de Banda de Entrada de Túnel (Rx) e Saída de Túnel (Tx) individual de cada Túnel com base no throughput bruto dos túneis na frequência desejada.
3. A solução pode ser capaz de calcular KPIs personalizados para fornecer a utilização de largura de banda de entrada (Rx) e saída de túnel (Tx) de cada pacote, que é a utilização de largura de banda agregada de todos os túneis entre um par de roteadores.
4. A solução pode detectar e criar alertas se os limites de nível de pacote definidos forem ultrapassados. Esses alertas estão disponíveis para monitoramento.
5. O alerta deve resultar no acionamento de um fluxo de trabalho automatizado que pode disparar ainda mais a configuração no dispositivo para adicionar ou remover túneis com base nas condições de alerta.
6. Finalmente, o sistema deve fechar automaticamente os alertas com as atualizações necessárias.

Solução

A solução de automação de loop fechado envolve várias ferramentas que trabalham com o objetivo específico nessa solução completa. Esta imagem mostra quais componentes e ferramentas nos ajudam a alcançar a arquitetura final e descreve a função de alto nível. Você pode observar cada componente e seu uso nas seções subsequentes.



Solução

Cisco Closed Loop Automation

Solução Cisco Closed Loop Automation

Ferramenta	Propósito
Cisco Crosswork Network Controller (CNC)	O Crosswork Network Controller permite visibilidade em tempo real do ciclo de vida do serviço e do dispositivo, com navegação intuitiva na topologia da rede, inventário de serviços, políticas de transporte, integridade do serviço, integridade do dispositivo e muito mais, oferecendo suporte a uma variedade de casos de uso com uma experiência de usuário comum e integrada. Nesta solução, ele é usado como uma ferramenta principalmente para o gerenciamento de dispositivos e coleta de dados de desempenho de túnel usando gNMI (gRPC Network Management Interface) ou MDT. Mais detalhes: https://www.cisco.com/site/us/en/products/networking/software/crosswork-network-controller/index.html
Matriz da Cisco	Os serviços de análise CX (pacotes de funções) são fornecidos com a solução Matrix, que é uma solução de análise de vários domínios e um único painel de controle de vários fornecedores. Nesta solução, a Matriz consome os dados do Kafka enviados pelo CNC sobre os

	Tópicos do Kafka e executa ainda mais a agregação de KPI baseado em túnel no KPI de nível de Pacote usando pesquisas de topologia e armazená-lo como dados de série temporal e armazená-lo no Banco de Dados Postgres. Uma vez armazenados, esses dados ficam disponíveis para visualização e a Matrix possui detecção de anomalias usando alertas de cruzamento de limites, o que nos permite configurar limites para os KPIs que coletamos da rede.
Cluster de Kafka	Um cluster de Kafka é um sistema que compreende diferentes tópicos de corretores, e suas respectivas partições. Um produtor envia ou grava dados/mensagens no tópico dentro do cluster. Um consumidor lê ou consome mensagens do cluster Kafka. Nesta solução, o CNC atua como o Produtor que envia dados para tópicos Kafka predefinidos na forma de payload JSON após converter dados de Telemetria coletados de roteadores. Nessa solução, a Matrix atua como o Consumidor que consome esses dados, processa os dados, os agrega e os armazena para processamento posterior e detecção de anomalias.
Cisco NSO	Cisco Crosswork Network Services Orchestrator (NSO) O NSO faz parte do portfólio Crosswork de ferramentas de automação criadas para provedores de serviços e grandes empresas. Nesta solução, o NSO coleta informações relacionadas a todos os túneis e dispositivos e cria uma tabela de topologia personalizada para esta solução. Além disso, nessa solução, o NSO, juntamente com os recursos de automação de processos de negócios, é usado para acionar um fluxo de trabalho de remediação e tomar medidas como adicionar ou remover um túnel do dispositivo e limpar mais os alertas no Cisco Matrix. Mais detalhes: https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
AIOps Vitria VIA	O Vitria VIA AIOps for Cisco Network Automation oferece análise automatizada que permite a rápida correção de eventos que afetam os serviços em todas as camadas de tecnologia e aplicativos. Nessa solução, os AIOps da VIA são usados para correlacionar eventos de limite de KPI gerados pelo Cisco Matrix, criar um incidente, uma notificação e acionar uma ação automatizada no Cisco NSO para aumentar ou diminuir a contagem de túnel GRE. Mais detalhes: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-

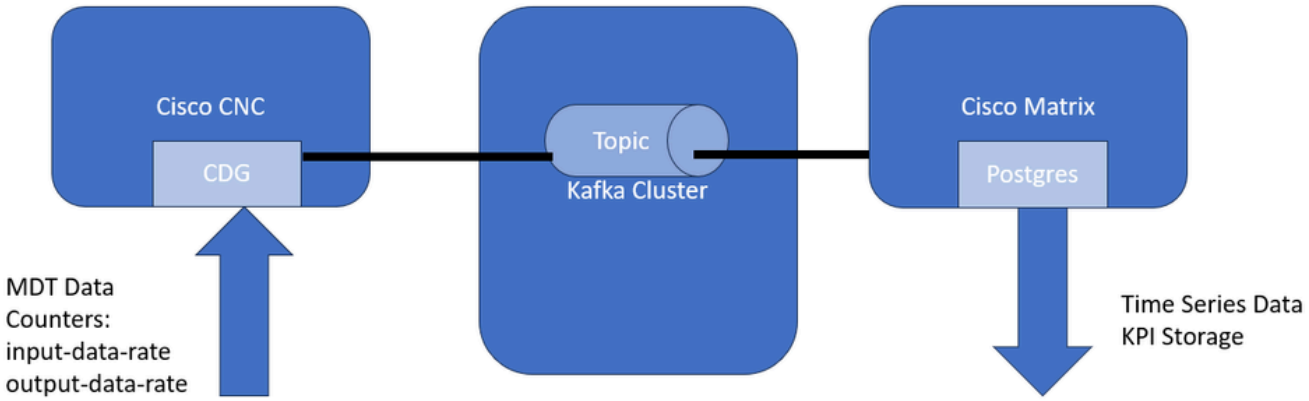
	management/crosswork-network-automation/solution-overview-c22-2403404.html

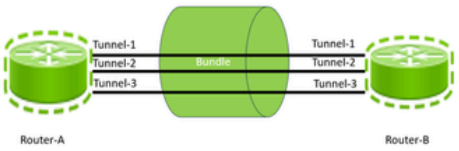
A solução segue estas etapas para preencher este caso de uso, que são elaboradas nas seções subsequentes.

1. Monitorar a utilização de túnel entre pares de roteadores
2. Monitorar a utilização de pacotes entre pares de roteadores
3. Criar alertas de cruzamento de limites
4. Desencadear o fluxo de trabalho de reparo automatizado e de incidentes
5. Adicionar ou remover túneis e limpar o alerta

Monitorar a utilização de túnel entre pares de roteadores

Os aplicativos solicitam a coleta de dados por meio de trabalhos de coleta. Em seguida, o Cisco Crosswork atribui esses trabalhos de coleta a um Cisco Crosswork Data Gateway para atender à solicitação. O Gateway de Dados de Trabalho Cruzado suporta a coleta de dados de dispositivos de rede usando a Telemetria Controlada por Modelo (MDT - Model-driven Telemetry) para consumir fluxos de telemetria diretamente de dispositivos (somente para plataformas baseadas no Cisco IOS XR). O Cisco Crosswork permite que você crie destinos de dados externos que podem ser usados por trabalhos de coleta para depositar dados.O Kafka pode ser adicionado como novos destinos de dados para trabalhos de coleta criados pela API REST. Nesta solução, o CDG coleta dados dos roteadores relacionados às estatísticas da interface do túnel e envia os dados para o tópico do Kafta. O Cisco Matrix consome os dados do tópico do Kafka e atribui os dados ao aplicativo do trabalhador da matriz que processa os dados como um KPI e os salva de uma maneira de série de tempo, como mostrado na figura subsequente que descreve o fluxo do processo.





Time	Node	KPI	Index	Value
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-1	1000
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-2	1200
22-05-2024 10:00:00	Router-A	input-data-rate	Tunnel-3	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-1	1400
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-2	1234
22-05-2024 10:00:00	Router-B	input-data-rate	Tunnel-3	1345

Os dados da série de tempo têm atributos KPI que são armazenados no Banco de Dados de Matriz.

Atributos de KPI	Propósito
Nó	O dispositivo ou Origem para o qual o KPI é armazenado Exemplo: Roteador A
Tempo	A hora em que os dados são coletados Exemplo: 22-05-2024 10:00:00
Índice	Identificador exclusivo Exemplo: Tunnel-1
Valor	Valor do KPI - Valor Numérico
KPI	Nome do KPI Exemplo: utilização de túnel

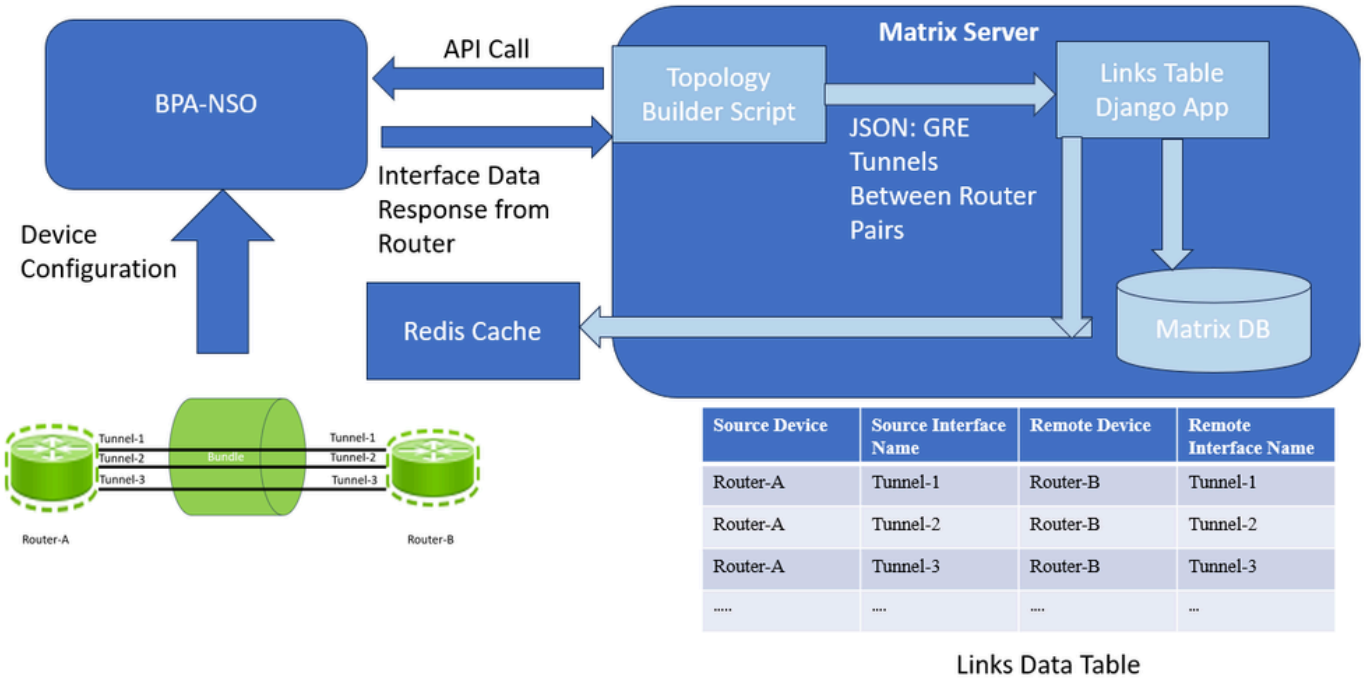
Monitorar a utilização de pacotes entre pares de roteadores

Quando você tiver os dados da série Time como mencionado na seção anterior, você terá as estatísticas de tráfego coletadas por interface de túnel. No entanto, você precisa identificar com qual dispositivo a interface de túnel de origem está conectada a qual outro dispositivo e qual é o nome da interface remota. Isso é chamado de Identificação de link, onde você identifica o Nome do dispositivo de origem. Source Interface Name (Nome da interface de origem), Remote Device Name (Nome do dispositivo remoto) e Remote Interface Name (Nome da interface remota). Para interpretar com precisão as informações do link e os roteadores, você precisa de um exemplo de referência conforme descrito.

Dispositivo de Origem	Nome da interface de origem	Dispositivo remoto	Nome da interface remota
Roteador-A	Túnel-1	Roteador B	Túnel-1
Roteador-A	Túnel-2	Roteador B	Túnel-2

Roteador-A	Túnel-3	Roteador B	Túnel-3
....	..	..	..

Para criar essa tabela de links de topologia nessa solução, você pode preencher uma tabela personalizada, Tabela de Dados de Links, criada na Matriz com base em um script executado no servidor todos os dias no horário preferencial. Esse script faz uma chamada de API para BPA-NSO e obtém uma saída JSON de pacotes GRE entre pares de roteadores. Em seguida, ele analisa os dados da interface para criar a topologia no formato JSON. O script também pega essa saída JSON e a grava na Tabela de dados de links todos os dias. Sempre que carrega os novos dados na tabela, ele também grava esses dados em um cache Redis para reduzir mais pesquisas no banco de dados e melhorar a eficiência.



Processo de Tabela de Dados de Links

Portanto, necessariamente todos os links entre os mesmos dois dispositivos são parte do pacote identificado como pertencente ao mesmo pacote.Assim que os KPIs de nível de túnel bruto estiverem disponíveis, você terá criado um aplicativo KPI_aggregate personalizado em Matrix, que executa o trabalho de calcular as utilizações de nível de pacote e armazená-las como um KPI.

Esse aplicativo recebe estas informações:

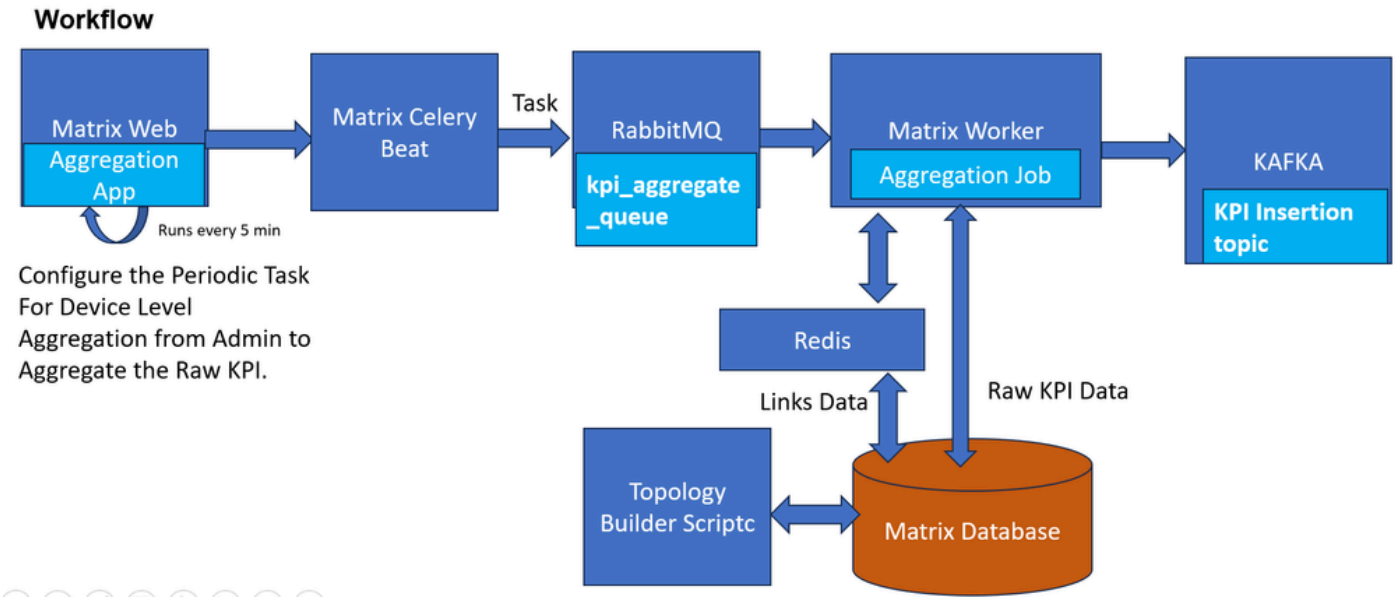
Atributo de configuração	Propósito

CrontabName	A frequência na qual a tarefa periódica de agregação deve ser executada
Caixa de seleção Habilitada	Ativar/Desativar esta configuração
Nome KPI da Interface do Túnel	Nome do KPI Bruto usado para calcular o KPI agregado. O Nome do KPI Agregado é criado automaticamente como <Raw_KPI_Name>_agg
Intervalo de datas	A frequência dos dados brutos.

A tarefa Agregar obtém as entradas do banco de dados de dados KPI Brutos e Links identifica os túneis que formam parte do mesmo pacote e os adiciona a um grupo com base nessa lógica.

```
KPI Name: <Raw_KPI_Name>_agg

Example: tunnel_utilization_agg

Value = sum (tunnel_interface_tx_link_utilization of all the interfaces on the device connected to same

Index: <local device> _<remote device>

Router-A _Router-B

Node: <Local-Device>

Router-A
```

Por exemplo, nesse caso, o nome do KPI é gerado como "tunnel-usage_agg" para a utilização de túnel KPI de Túnel bruto. Quando o cálculo for concluído para todos os valores de KPI brutos de todos os roteadores e combinações de túnel, esses dados serão enviados para cada link do tópico do Kafka, que deve ser o mesmo tópico que ingere o KPI processado. Dessa forma, essas informações persistem como qualquer outro KPI normal recebido de fontes válidas. O consumidor do BD consome a partir deste tópico e persiste o KPI na tabela de resultados de KPI no Banco de Dados de Matriz para os KPIs agregados.



Processo de Agregação de KPI para KPI Agregado no Nível do Pacote

Criar alertas de cruzamento de limites

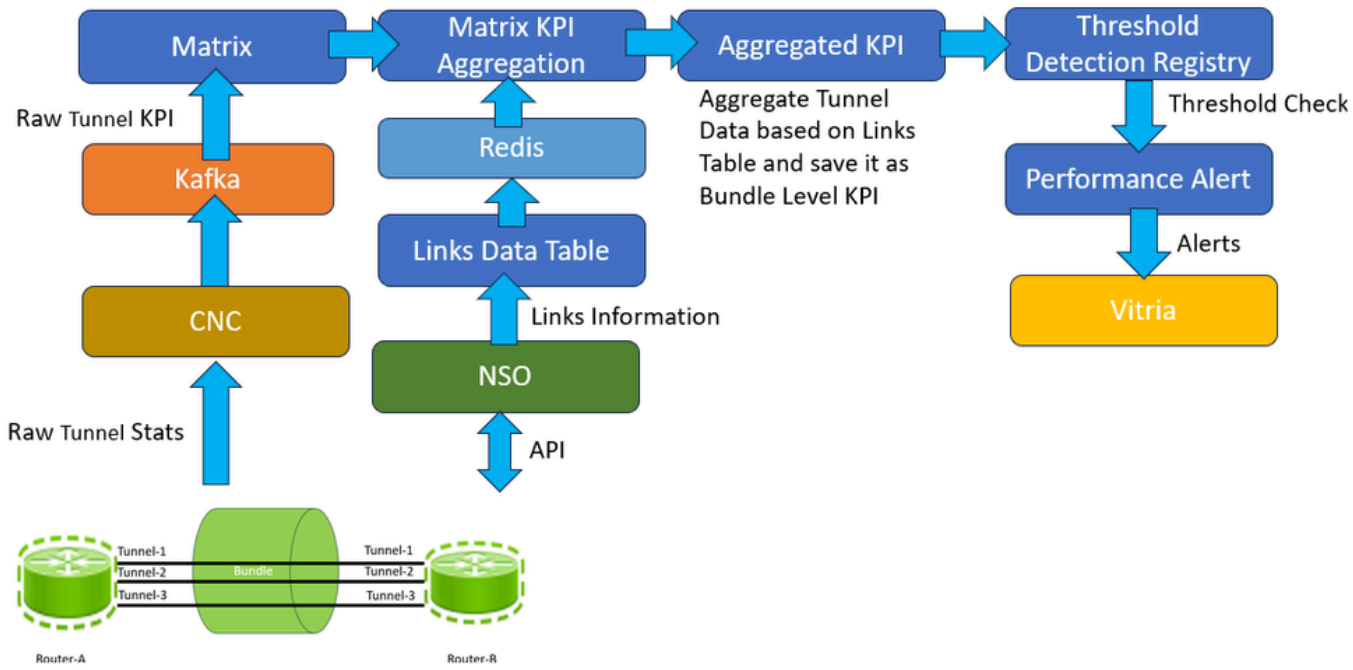
O limite de KPI configurado na Matriz é de 85%, o que significa que quando o valor desse KPI excede o limite, um alerta crítico é gerado e, quando ele diminui abaixo do limite, um alerta claro é gerado. Esses alertas são salvos no banco de dados da matriz e também encaminhados para a Vitria nesta solução para o caso de uso de automação de loop fechado. Se o valor calculado do KPI ultrapassar o limite, um alerta será enviado para Vitria (VIA-AIOPs) via Kafka com o estado atual como Crítico na mensagem. Da mesma forma, se o valor retornar dentro dos valores de limite a partir dos valores críticos, ele deve enviar um alerta para VIA-AIOPs via Kafka com o estado atual como Clear na mensagem. Uma mensagem de exemplo foi enviada ao sistema e seus atributos são os seguintes.


```
{
   "nó": "Roteador-A",
   "node_type": "Roteador",
   "kpi": "tunnel_usage_agg",
   "kpi_description": " Utilização em nível de pacote",
   "esquema": "",
   "index": "Router-A_Router-B",
   "tempo": "08-08-2023 05:45:00+00:00",
   "valor": "86,0",
   "previous_state": "LIMPAR",
```

<table>
<tr><td colspan="3">"current_state": "CRÍTICO",
"link_name": "Roteador-A_Roteador-B"
}</td></tr>
<tr><td>Atributo de mensagem de alerta Kafka</td><td>Exemplo de valor</td><td>Propósito</td></tr>
<tr><td>nó</td><td>Roteador-A</td><td>Nome do dispositivo de rede</td></tr>
<tr><td>node_type</td><td>Router</td><td>tipo de dispositivo</td></tr>
<tr><td>KPI</td><td>tunnel_usage_utilização</td><td>Nome do KPI</td></tr>
<tr><td>kpi_ description</td><td>Utilização de nível de pacote</td><td>Descrição do KPI</td></tr>
<tr><td>Esquema</td><td>NA</td><td>NA</td></tr>
<tr><td>índice</td><td>Roteador-A_Roteador-B</td><td><dispositivo_local>-
<dispositivo_remoto></td></tr>
<tr><td>tempo</td><td>"2023-08-09
05:45:00+00:00"</td><td>tempo</td></tr>
<tr><td>valor</td><td>86.0</td><td>valor de KPI</td></tr>
<tr><td>estado_anterior</td><td>CLEAR</td><td>Estado anterior de alerta</td></tr>
<tr><td>estado_atual</td><td>CRÍTICO</td><td>Estado atual de alerta</td></tr>
<tr><td>link_name</td><td>Roteador-A_Roteador-B</td><td>Atributo de correlação</td></tr>
</table>

o atributo link_name é um nome classificado alfabeticamente dos dispositivos presentes no valor de índice. Isso é feito para obter correlação no nível VIA AIOPs, em que VIA AIOps deve correlacionar os alertas provenientes do mesmo link de pacote. Por exemplo, quando vários alertas estão chegando aos AIOPs VIA com o mesmo link_name, isso significa que os alertas

pertencem ao mesmo link de pacote na rede denotado por nomes de dispositivo no nome do link.



Geração de Alerta de Agregação de KPI usando o Registro de Detecção de Matriz

Desencadear o fluxo de trabalho de reparo automatizado e de incidentes

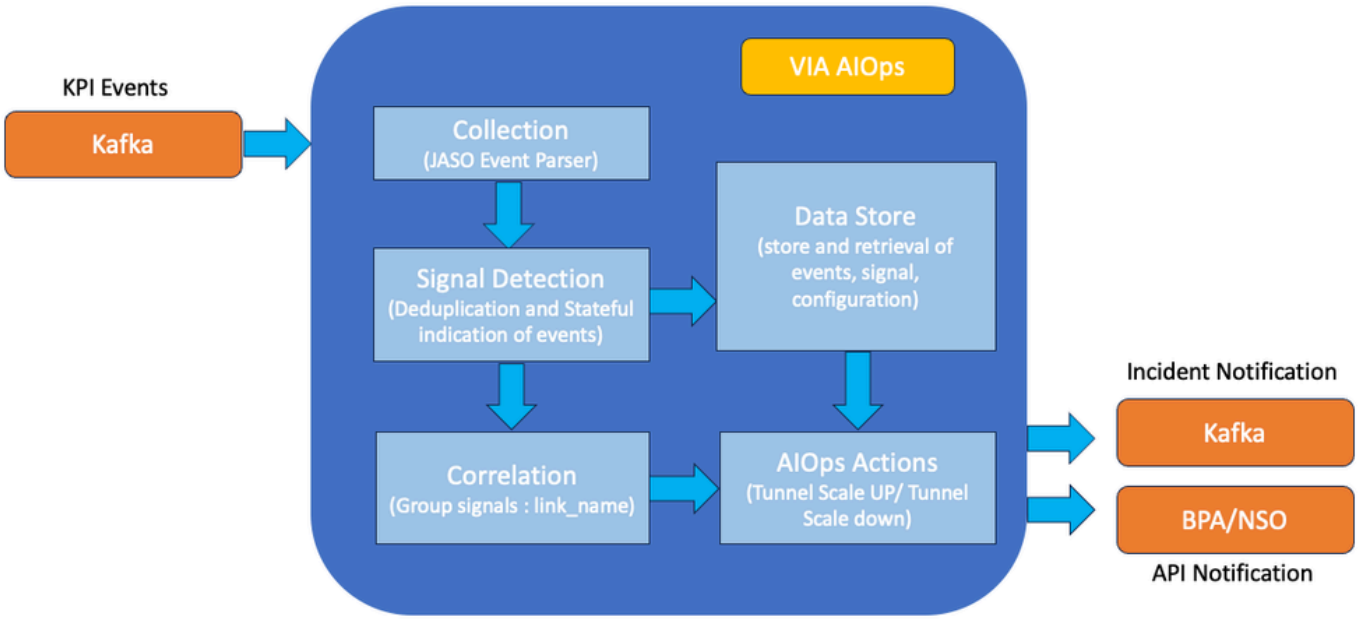
Através de AIOps deve ser configurado para a inclusão de eventos de anomalia do Indicador Chave de Desempenho (KPI) de um tópico Kafka designado. Esses eventos, como recebidos por meio de mensagens Kafka, são processados pelos AIOps da VIA através do analisador de eventos do JASO para inclusão subsequente. É essencial que os AIOps da VIA identifiquem precisamente os eventos de anomalia de KPI relacionados aos túneis GRE, determinem sua associação com pares de dispositivos específicos (por exemplo, Roteador A - Roteador B) e verifiquem se a anomalia requer o início da automação de escala de túnel GRE — seja em upscale ou downscale.

O Analisador de Eventos JASO nos AIOps VIA deve ser configurado para extrair e interpretar dimensões relevantes do evento de anomalia de KPI de Matriz, ou seja, o ‘host’, o 'kpi', o 'índice' e o 'valor'. Uma dimensão adicional, denominada 'automation_action', deve ser configurada para ser atualizada dinamicamente pelo analisador de eventos JASO, com base na métrica 'value' presente no evento de anomalia Matrix KPI. Essa dimensão é essencial para determinar se uma resposta automatizada deve ser decretada, especificamente para disparar procedimentos de "Escala de Túnel GRE Superior" ou "Escala de Túnel GRE Inferior", processando o campo "valor de KPI". Em VIA AIOps, um sinal representa uma consolidação dos estados dos eventos. Para aprimorar esse processo de correlação, devemos configurar sinais stateful distintos que se correlacionam às dimensões 'host', 'link name', 'kpi' e 'automation_action'. A tabela exemplifica os sinais, os grupos de correlação e suas respectivas configurações de correlação.

Por exemplo, o sinal identificado como GRE_KPIA_SCALEUP seria iniciado após a inclusão de uma mensagem de anomalia de KPI especificada, conforme detalhado na Seção 3, pelo sistema VIA AIOps.

Nome do sinal VIA AIOps	Chaves de correlação de sinal	Nome da regra do grupo de correlação
GRE_KPIA_SCALEUP	Host,kpi, Nome do link, Ação_automática	Dimensionamento vertical de túnel GRE
GRE_KPIB_SCALEUP	Host,kpi, Nome do link, Ação_automática	
GRE_KPIA_SCALEDOWN	Host,kpi, Nome do link, Ação_automática	Escala de túnel GRE
GRE_KPIB_SCALEDOWN	Host,kpi, Nome do link, Ação_automática	

A regra do grupo de correlação é projetada para facilitar a agregação de sinais sobre o dispositivo A, o dispositivo B e seus respectivos túneis A, B e C em um incidente unificado. Essa regra de correlação garante que, para qualquer emparelhamento específico do Dispositivo A e do Dispositivo B, um máximo de dois incidentes distintos seja gerado: um incidente para uma expansão de túnel GRE envolvendo o Dispositivo A e o Dispositivo B, e outro incidente para uma redução de túnel GRE para o mesmo emparelhamento de dispositivos. A estrutura do agente VIA AIOps é capaz de fazer interface com o Business Process Automation (BPA) e o Network Services Orchestrator (NSO).



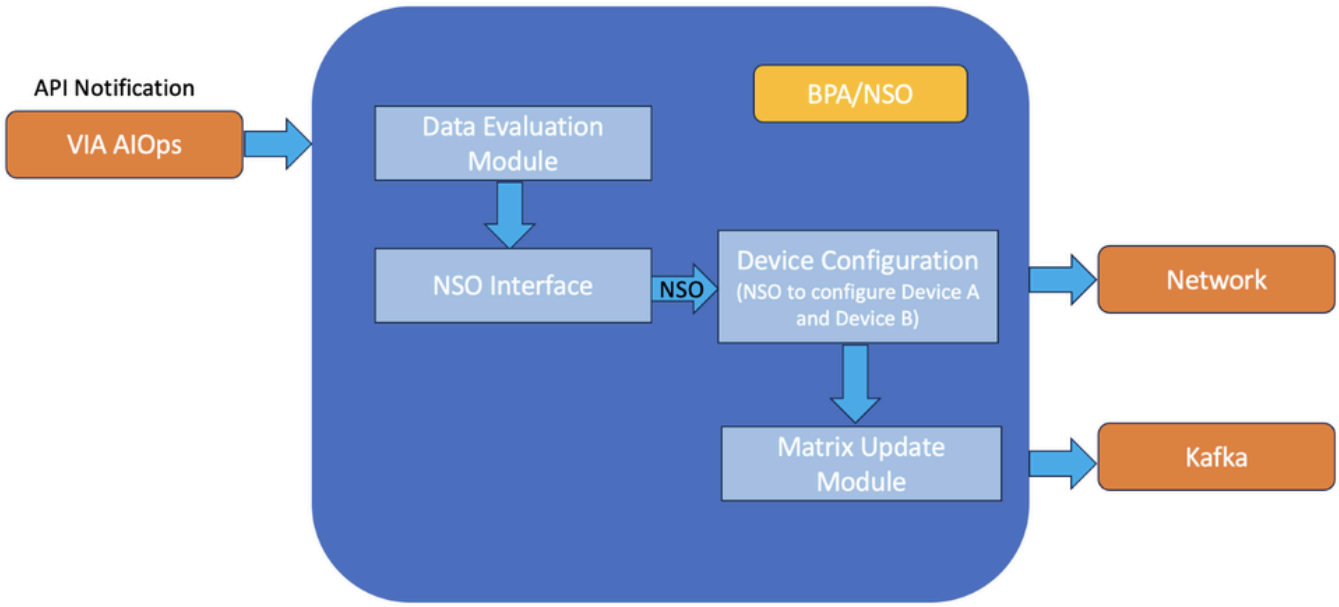
Correlação e Notificação de Evento KPI usando VIA AIOps

Este é um exemplo de uma notificação de API de ajuste de escala vertical de túnel GRE enviada para BPA/NSO de VIA AIOps.

```
{
  "create": [
    {
      "gre-tunnels-device-cla": [
        {
          "index": "RouterA-RouterB",
          "tunnelOperation": "SCALE UP",
          "MatrixData": [
            { "node": "RouterA", "kpi": "tunnel_utilization_agg" },
            { "node": "RouterB", "kpi": "tunnel_utilization_agg" }
          ]
        }
      ]
    }
  ]
}
```

Adicionar ou remover túneis e limpar o alerta

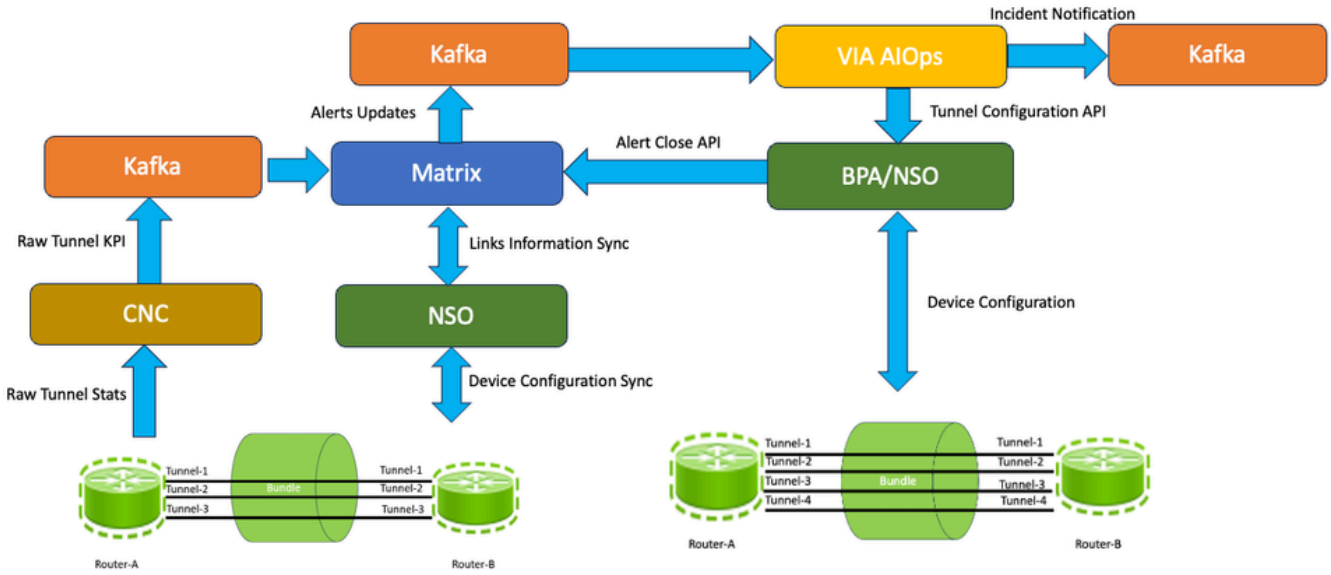
Ao receber uma chamada de API de VIA AIOps, o Cisco Business Process Automation (BPA) inicia as diretivas de dimensionamento necessárias, por meio de solicitações internas ao Cisco Network Service Orchestrator (NSO). O BPA avalia o payload de dados fornecido pelos AIOps da VIA, que inclui detalhes da operação de túnel, um índice e dados de matriz. As informações de operação de índice e túnel são utilizadas para fazer interface com o NSO, fornecendo parâmetros para a operação de escala. Simultaneamente, os Dados de Matriz são processados pelo 'Módulo de Atualização de Matriz', que é responsável por resolver quaisquer eventos de anomalia de KPI através de interface com as APIs de Matriz.



Validação de dados e configuração de dispositivo usando BPA-NSO

Antes de iniciar qualquer operação de escalonamento, é necessário desenvolver um modelo de ação YANG para o NSO. Esse modelo define as ações específicas que o NSO deve executar para aumentar ou diminuir a contagem de túnel entre o Roteador A e o Roteador B. O sistema BPA (Business Process Automation, automação de processos de negócios) começa a dimensionar as operações ao se envolver com o NSO (Network Service Orchestrator, orquestrador de serviços de rede) para realizar uma "simulação". Esta é a fase inicial da operação em que o BPA solicita que o NSO simule as alterações de configuração pretendidas sem aplicá-las. A simulação funciona como uma etapa de validação essencial, garantindo que as ações de dimensionamento propostas, conforme definido pelo modelo de ação YANG, possam ser executadas sem causar erros ou conflitos na configuração da rede.

Se a simulação for considerada bem-sucedida, indicando que as ações de dimensionamento foram validadas, o BPA então avança para o estágio de "confirmação". Neste ponto, o BPA instrui o NSO a implementar as modificações de configuração reais necessárias para aumentar ou diminuir a contagem de túnel GRE entre o Roteador A e o Roteador B. O BPA aciona o 'Módulo de atualização de matriz' em direção à matriz usando uma chamada de API para fechar o evento de KPI em conjunto com os AIOps da VIA. Quando essa anomalia é fechada na Matrix, a Matrix também envia um alerta com gravidade como "Removido" para os AIOps da VIA, o que fecha ainda mais o incidente em sua extremidade. Dessa forma, o ciclo de remediação em nível de rede é concluído. Uma versão generalizada do fluxo de dados no aplicativo, utilizada nessa automação de loop fechado, é ilustrada nesta imagem.



Fluxo de dados para um pacote de túnel GRE com automação de loop fechado

Fechando o loop para abrir novas possibilidades de correção automática

A solução discutida neste documento é discutida deliberadamente com um exemplo de dimensionamento do pacote GRE com base em anomalias de rede para nos ajudar a nos relacionar com vários blocos de construção desta solução. É estudado resumidamente como o Cisco Technology Stack, que inclui o Cisco NSO, o Cisco Matrix e o Cisco BPA, pode se integrar perfeitamente a componentes como VIA AIOps, Kafka e outra pilha de software para nos ajudar a monitorar e corrigir automaticamente problemas de rede. Essa solução abre possibilidades para todos os outros casos de uso de rede, que podem ser problemas típicos que ocorrem no provedor de serviços ou nas redes corporativas.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.