CONTROLE DE BANDA EM ENLACES WAN UTILIZANDO QUALITY OF SERVICE (QoS) E LISTAS DE ACESSO TEMPORAIS: ATUALIZAÇÕES DE SERVIÇOS DE REDE

Diogo César Dantas Fernandes

Orientador: Gilles V. T. Silvano

RESUMO

Este documento trata de um estudo sobre como controlar o congestionamento de enlaces de rede WAN (*Wide Area Network*) provocados por atualizações de Sistemas Operacionais Microsoft que utilizam a plataforma de atualização WSUS (*Windows Server Update Service*) e também de atualizações de antivírus Symantec. Utilizando QoS (*Quality of Service*) associado com listas de acesso temporal é possível marcar e policiar atualização de tais serviços de acordo com uma política de tráfego específica, dependendo do horário em que a transferência ocorre, proporcionando que em horários comerciais ou estipulados pelos clientes as atualizações das plataformas referidas não comprometam o funcionamento de sistemas fins ou mais prioritários. Esta solução já foi implementada nacionalmente para determinado órgão do governo federal, onde foi obtido um resultado satisfatório, medido e acompanhado por ferramentas de gerência e desempenho de rede, não sendo mais observada a ocorrência de grandes fluxos de atualização nos enlaces de rede WAN fora dos horários permitidos e designados para este fim.

Palavras-Chave: Projeto de Redes WAN. QoS. ACL temporal. WSUS. Antivírus.

WAN LINK BAND CONTROL USING QUALITY OF SERVICE (QoS) AND TIME ACCESS LISTS: NETWORK SERVICE UPDATES

ABSTRACT

This article is about a study on how to control the congestion of Wide Area Network (WAN) links caused by updates of Microsoft Operating Systems that use the Windows Server Update Service (WSUS) update platform as well as Symantec antivirus updates. Using Quality of Service (QoS) associated with temporary access lists, it is possible to mark and polish the updating of such services according to a specific traffic policy, depending on the time the transfer takes place, providing that at business hours or stipulated by clients the Upgrades of the referred platforms do not compromise the operation of systems purposes or more priority. This solution has already been implemented nationally for a certain federal government agency, where a satisfactory result has been obtained, measured and accompanied by management tools and network performance, no longer observing the occurrence of large update flows in the WAN network links outside the Designated times for this purpose.

Keywords: WAN Network Design. QoS. Time ACL. WSUS. Antivirus.

1 INTRODUÇÃO

Os ambientes corporativos de TI (*Technology Information*) possuem inúmeros serviços de rede que dão suporte as mais diversas aplicações e necessidades dos usuários. Alguns desses serviços, ou plataformas, precisam ser constantemente atualizados para funcionarem bem. É o caso dos sistemas operacionais, aplicações e agentes de segurança, que requerem atualizações frequentes. Normalmente essas atualizações são realizadas através da transferência de médios ou grandes arquivos de dados, que consequentemente demandam grandes larguras de banda nas infraestruturas de rede WAN. Dependendo do tamanho, do horário e dia em que a atualização ocorre, a largura de banda dos enlaces de rede WAN pode se tornar insuficiente, gerando concorrência entre aplicações e serviços mais prioritários. Pensando nesta possível problemática, o QoS, trabalhando em conjunto com a lista de acesso temporal, se mostraram como uma solução simples e viável para permitir que as atualizações de antivírus e WSUS sejam marcadas e policiadas de acordo com uma política de tráfego específica, dependendo do horário em que o tráfego ocorre.

2 FUNDAMENTOS DE WSUS, ANTIVÍRUS E QoS

Segundo a Microsoft (2017), O WSUS permite que os analistas e técnicos de tecnologia da informação realizem as atualizações necessárias, de forma automática ou agendada, dos produtos da Microsoft. Com o WSUS, as atualizações lançadas pelo Microsoft *Update* podem ser gerenciadas e distribuídas totalmente entre os computadores na rede.

O servidor do WSUS é capaz de realizar as tarefas de atualização por meio de um console de gerenciamento, além de poder ser a fonte de atualização de outros servidores do WSUS na organização. O servidor do WSUS que atua como fonte de atualização é chamado de servidor *upstream*. Pelo menos um servidor do WSUS na rede precisa se conectar ao Microsoft *Update* para obter as informações de atualizações disponíveis, mas o administrador pode determinar, com base na segurança, disponibilidade e largura de banda da rede, quantos outros servidores se conectam diretamente ao Microsoft *Update*.

O gerenciamento de atualizações ajuda a manter a eficiência operacional dos serviços de TI, controlar vulnerabilidades de segurança e manter a estabilidade do seu ambiente de produção e serviços de rede. Um ambiente desatualizado em seus sistemas operacionais e aplicativos, pode gerar inúmeras vulnerabilidades de segurança que, se exploradas por *hackers*, poderão resultar na perda de dados, confiabilidade e disponibilidade da informação. A instalação de atualizações e *patches* recomendados compõem uma dos pilares das boas práticas de segurança, eficiência e disponibilidade dos sistemas de tecnologia. As principais vantagens do WSUS são:

- Gerenciamento centralizado de atualizações
- Automação do gerenciamento de atualizações

As atualizações do WSUS, tanto para servidores, quanto para clientes, podem ocorrer tanto de forma manual, como de forma automática. Para o caso de ser automático, pode-se definir uma agenda de sincronização, onde poderá ser definido os dias, horários e frequência de atualização.

No caso dos servidores, configura-se o servidor de *upstream* (Microsoft *Update* ou outro servidor WSUS) e a forma de atualização, manual ou automática. Para o caso de ser automática, configura-se também a frequência que são checadas novas atualizações no dia.

Para o caso dos clientes, as atualizações também podem ocorrer de forma manual ou automática. Para o caso de ser automática, a configuração de atualização estará inserida dentro da política de grupo de um domínio atribuída a estação, contida e administrada pelo serviço de diretório *Active Directory*. É possível também aplicar a configuração de atualização automática em um cliente não controlado pelo *Active Directory*, através da edição das políticas locais da estação, fazendo o apontamento correto para os servidores de WSUS.

Através de uma política de grupo criada para o WSUS, onde estejam inseridas as estações que se deseja automatizar as atualizações, podem ser inseridas as seguintes possibilidades de configuração:

- **Avisar antes de baixar e de instalar qualquer atualização:** Esta opção notifica um usuário administrativo conectado antes de baixar e instalar as atualizações.
- **Baixar automaticamente e notificar antes de instalar:** Esta opção começa automaticamente a baixar as atualizações e notifica um usuário administrativo conectado antes de instalá-las. Por padrão, essa opção é selecionada.
- **Baixar automaticamente e agendar a instalação:** Esta opção começa automaticamente a baixar as atualizações e as instala no dia e hora que você especificar.
- **Permitir que o administrador local escolha a configuração:** Esta opção permite que administradores locais usem as Atualizações Automáticas do Painel de Controle para escolher uma opção de configuração. Por exemplo, eles podem optar por agendar uma instalação. Os administradores locais não podem desabilitar as Atualizações Automáticas.

Assim como o WSUS, o serviço de antivírus Symantec corporativo utiliza o modelo cliente servidor para realizar as atualizações. As estações, através de agentes de antivírus, solicitam e baixam suas atualizações de servidores estrategicamente posicionados na rede, de forma que o tráfego de dados possa ser distribuído e replicado sem impactar as bandas dos enlaces de rede WAN. Normalmente são instalados servidores nas redes locais, que replicam as atualizações de outros servidores *upstream* de antivírus, que por sua vez, recebem as atualizações de servidores da Symantec conectados à Internet.

O QoS, também chamado de qualidade de serviço, é uma tecnologia que permite que pacotes IP (*Internet Protocol*) possam ser tratados e encaminhados pelos dispositivos de rede de forma diferenciada, um dos outros, de acordo com os mais variados tipos de tráfego e políticas de transmissão de uma rede. Este tipo de recurso tem sido bastante empregado nos últimos tempos, com a convergência de serviços, principalmente quando os enlaces de rede WAN passaram a compartilhar bandas que eram exclusivas de pacotes de dados, com pacotes de voz e vídeo.

Basicamente o QoS se baseia em três conceitos para realizar de forma eficiente a sua função: Classificação e marcação, gerenciamento de congestionamento e controle de admissão.

1. Classificação e marcação: selecionar o tráfego, separá-lo por tipos de aplicações e marcá-lo com um campo que permite a todos os roteadores identificar à qual classe esse tráfego pertence é a base de todo o processamento do QoS. Dependendo do tipo de interface em questão e das características do equipamento, a marcação pode ser feita na camada dois (802.1p/q), na camada três (IP *Precedence* ou *Differentiated Services Code Point (DSCP))* ou no *label* MPLS (*Multiprotocol Label Switching*) Campo *Experience (EXP)*.
2. Gerenciamento de congestionamento: existem alguns mecanismos para controle de fila e congestionamento, que utilizam algoritmos e métodos diferentes para criar e gerenciar as filas de transmissão. Dentre eles podemos citar o *Low Latency Queueing* (LLQ), *Weighted Fair Queueing* (WFQ) e o *Class-Based Weighted Fair Queueing* (CBWFQ).
    2.1. LLQ: este mecanismo cria uma fila de alta prioridade, que atua em conjunto com as filas de CBWFQ, com garantia e limitação de banda total permitida. Na presença de um único pacote nesta fila, o mecanismo de esvaziamento interrompe o atendimento às demais filas e transmite os pacotes desta fila, até o limite de banda definido. Pacotes que excedam esse limite somente serão transmitidos caso a interface não possua nenhum tipo de congestionamento.
    2.2. WFQ: esse mecanismo utiliza o algoritmo *Fair Queueing (FQ)* mas acrescenta uma variável a mais no cálculo do *Finish Time* dos pacotes. Esta variável é o peso ou prioridade atribuída a cada pacote. Pacotes com maior peso tendem a ter um menor *Finish Time* e, conseqüentemente, maior porção de banda alocada para o fluxo. Sendo assim, a alocação de banda deixa de ser puramente linear, como no FQ, e passa a ser ponderada conforme o peso atribuído aos pacotes de um fluxo. A prioridade de um pacote é atribuída conforme o

valor do *IP Precedence* ou *Differentiated Services Code Point (DSCP)* do cabeçalho IP.

2.3. CBWFQ: tem o mesmo princípio de funcionamento do WFQ, com a vantagem de permitir ao usuário definir as próprias classes de tráfego, limitado a até 64 classes. No WFQ as classes (filas) são criadas de forma automática e dinâmica com base nos fluxos de pacotes. Assim, o CBWFQ aumenta a flexibilidade do WFQ ao garantir um maior controle e refinamento das classes de tráfego, que podem ser criadas segundo critérios de classificação como listas de acesso, protocolos, endereço IP de origem e/ou destino, interface de entrada, entre outros. No CBWFQ o peso de cada classe é definido com base na banda alocada por classe. Esta é outra diferença do CBWFQ em relação ao WFQ, que define o peso de uma fila pelo IP Precedence do pacote. O CBWFQ ainda permite outras facilidades como a implementação de mecanismos de policiamento (*policing*) e a moldagem (*shaping*) por classe.

3. Controle de admissão: os mecanismos de policiamento utilizam um esquema de medição de tráfego denominado *Token Bucket*. Este esquema utiliza um conjunto de tokens que são colocados em um *bucket* a uma taxa constante. Cada *token* representa um crédito para transmissão de um *byte*. Um pacote só é transmitido quando há *tokens* suficientes no *bucket* para transmissão do pacote por inteiro. Quando um pacote chega à interface e não há *tokens* suficientes no *bucket* autorizando a transmissão, então é feita uma consulta a um *bucket* extra para verificar se há *tokens* adicionais para permitir a transmissão. Estes *tokens* adicionais representam a quantidade de *bytes* excedentes que podem ser transmitidos. No caso de se fazer uso do crédito de tokens excedentes, o pacote é remarcado com uma prioridade inferior antes de ser transmitido. Caso todos os créditos tenham se esgotados, então o pacote é descartado. Caso o *bucket* se encha de *tokens* e eles não sejam consumidos para transmitir pacotes, novos tokens são descartados. As características do *Token Bucket* são definidas pelos seguintes parâmetros:

3.1. *Time Interval* (Tc): define os intervalos de tempo de amostragem de tráfego. O valor do Tc é dado pela fórmula Tc = *Conformed Burst Size (Bc)* / *Committed Information Rate (CIR)*. O Tc define também a taxa com que os *tokens* são colocados no *bucket*.

3.2. *Conformed Burst Size (Bc)*: define o tamanho da rajada que corresponde à quantidade de *tokens* que cabem no *bucket*. Em outras palavras, o Bc determina a quantidade de tráfego que pode ser transmitido em um intervalo de tempo Tc. Este valor também é identificado como *Normal Burst Size* e é dado em *bytes*.

3.3. *Extended burst size* (Be): define a quantidade de tráfego excedente que pode ser transmitido acima do Bc num intervalo de tempo Tc. Também é dado em bytes.

3.4. *Mean rate*: taxa média de transmissão, também conhecida como *Committed Information Rate* (CIR), dada em *bits* por segundo (bps).

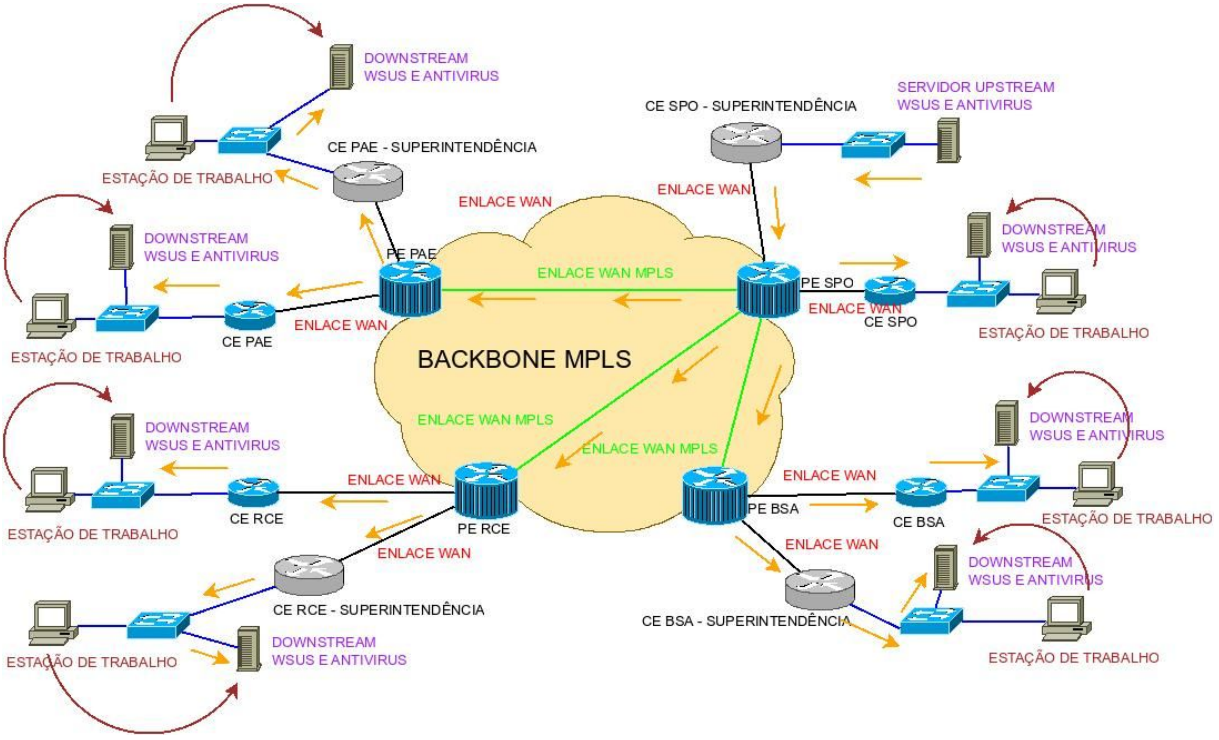
Como o comportamento do tráfego pode oscilar no decorrer do tempo, a quantidade de bits transmitidos a cada Tc pode variar acima ou abaixo de Bc.

3 DESCRIÇÃO DA PROBLEMÁTICA

Como já abordado no referencial teórico, as aplicações de WSUS e antivírus funcionam em um modelo cliente servidor. A topologia de funcionamento adotada por estes serviços na rede corporativa, foco do estudo deste documento, é baseada na distribuição de servidores *downstream* instalados e posicionados nas redes locais das diversas unidades, em âmbito nacional, que solicitam atualizações de replicação para os servidores de *upstream* instalados e posicionados geograficamente e logicamente em redes remotas, interligadas por meio de enlaces WAN. As estações de trabalho, por sua vez, atualizam-se através dos servidores *downstream* já mencionados, sempre com a última atualização disponível, utilizando-se de enlaces de rede local, as chamadas *Local Area Network (LAN)*, que normalmente utilizam switches com alta capacidade de largura de banda, conforme podemos observar na Figura 1. Nas LANs mais modernas essa largura de banda não é inferior a transmissões abaixo de 1Gbps. Pelo motivo da limitação de altas larguras de banda em enlaces WAN, e da maior oferta em LANs, sempre será mais eficiente distribuir e

replicar uma única atualização para os servidores de redes locais *downstream*, deixando estes responsáveis por gerenciar as atualizações das estações de trabalho.

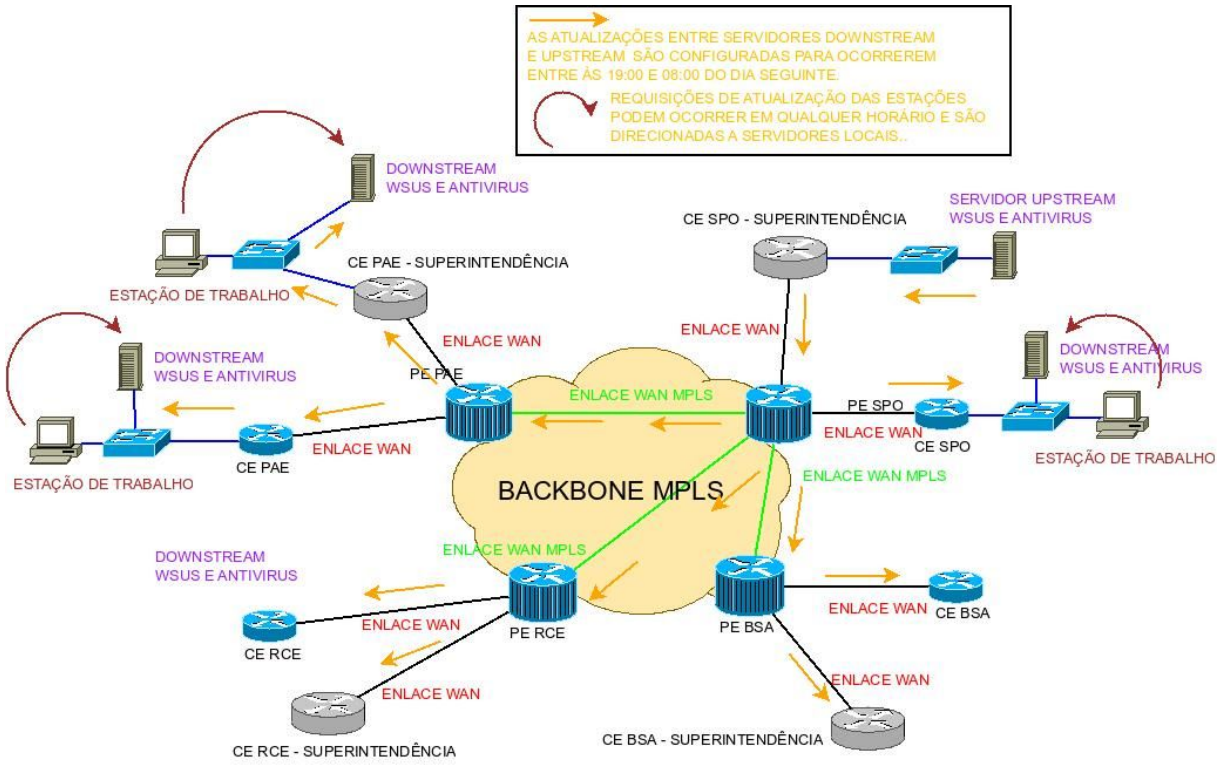
Figura 1. Topologia e fluxo de atualização dos serviços de WSUS e Antivírus. Ilustra como é realizado o fluxo de atualização das máquinas de *upstream* para *downstream*, assim como as requisições de atualização das estações para o servidores.



Fonte: Elaborada pelo autor (2017).

Mesmo que a topologia adotada e descrita favoreça a economia de banda das redes WAN, ainda assim é necessário prevenir que tais atualizações sejam realizadas nos momentos em que os usuários mais requerem por serviços e, por consequência também, mais largura de banda. Sendo assim, a periodicidade e a hora em que as replicações entre servidores e as atualizações das estações são realizadas compreendem horários não comerciais, normalmente à noite, entre às 19:00 e 08:00 da manhã do dia seguinte. Tal configuração no serviço de WSUS minimiza a possibilidade de ocorrência de esgotamento de banda em enlaces WAN durante os períodos de maior utilização dos usuários, conforme Figura 2.

Figura 2. A atualização dos serviços ocorre entre 19:00 e 08:00 do dia seguinte.



Fonte: Elaborada pelo autor (2017).

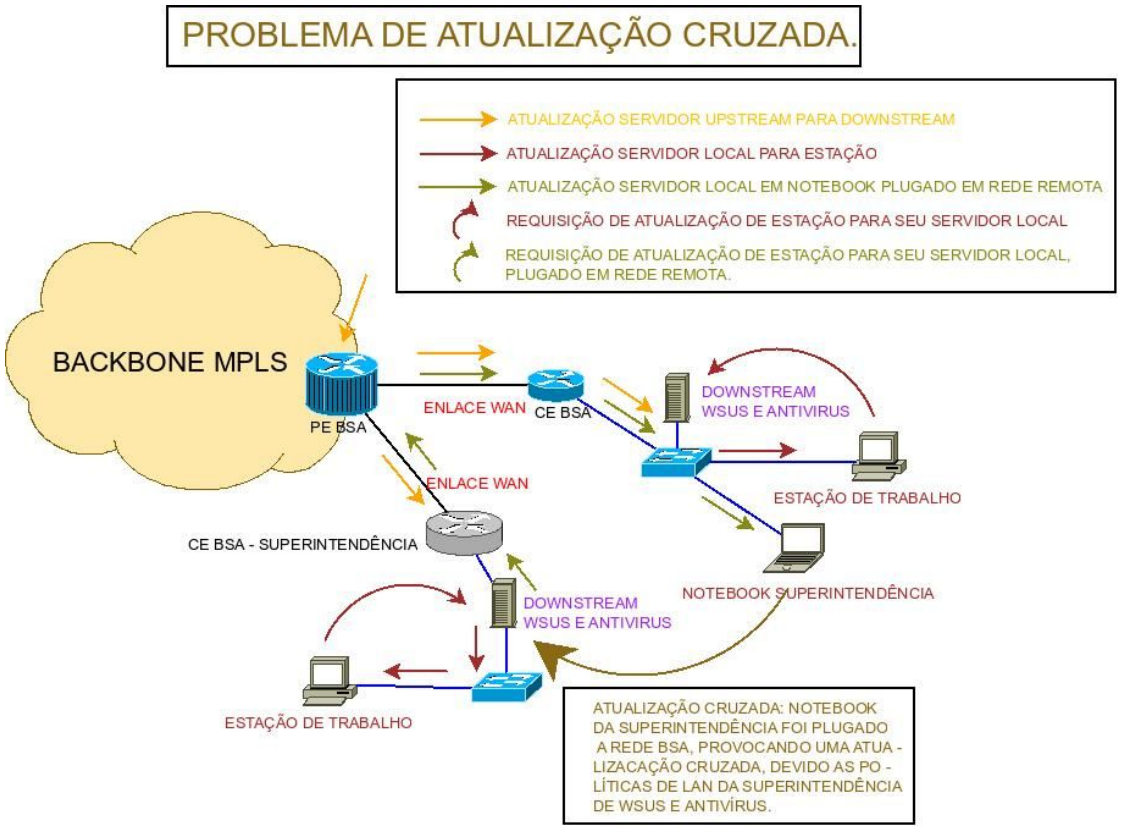
Ao contrário do WSUS, as atualizações do serviço de antivírus não podem ser restringidos a horários. Pela natureza e criticidade que produtos de segurança requerem, uma vez disponível uma atualização de segurança, a mesma imediatamente deve ser repassada para seus agentes. Tal política e, dependendo do tamanho da atualização, pode inundar os já escassos recursos de banda dos enlaces de rede WAN.

Ainda que a distribuição de servidores de *downstream* e o agendamento das atualizações sejam opções que de fato funcionam, alguns eventos e ou problemas podem ocorrer e gerar que as atualizações dos serviços ocorram em servidores remotos ou fora do horário programado. Alguns dos motivos são:

1. Erro de configuração: Quando o *script* de configuração da ferramenta das estações falha, ou por erro de configuração humana.
2. Falha no servidor de *downstream* instalado na rede local: Em caso de falha do servidor, as estações passarão a atualizar a partir de máquinas remotas.
3. Atualização cruzada: Ocorre quando uma estação ou *notebook* é plugado em uma LAN que faz parte da mesma organização, mas que não é a de origem

do equipamento. Devido às diretivas e políticas configuradas da LAN de origem, o dispositivo irá requerer também atualizações do servidor local de antivírus de origem, provocando tráfego nos *links* de WAN. A Figura 3 ilustra esta problemática. Exemplo: Usuário viaja a trabalho para outra unidade da organização e conecta o *notebook* a rede local diferente da de origem.

Figura 3. Problema da atualização cruzada.



Fonte: Elaborada pelo autor (2017).

4 POSSÍVEIS SOLUÇÕES

Para tratar os problemas apresentados, duas soluções seriam possíveis. A primeira delas seria implementar na origem e destino das atualizações o bloqueio de tráfego por meio de *firewalls*. A segunda seria criar uma política de QoS que fosse possível classificar o tráfego de rede do cliente e, a partir disso, elaborar um controle de filas de priorização e política de admissão de tráfego de acordo com os serviços utilizados.

De acordo com a topologia, a facilidade e os recursos já disponíveis, o QoS se mostrou uma solução mais completa e atrativa para a resolução do problema. As vantagens do uso de QoS em detrimento aos dos *firewalls* são:

- Recursos e equipamentos compatíveis com a tecnologia de QoS e disponíveis para configuração;
- Capacidade de estabelecer uma política de tráfego WAN nacional baseada nos principais serviços e necessidades dos cliente;
- Configurar e reservar larguras de banda por serviço;
- Limitar e controlar o tráfego das atualizações, mesmo em horários comerciais, sem a necessidade de bloquear o tráfego; e
- Sem investimentos.

As desvantagens do uso de *firewalls* são:

- Necessidade de realização de investimentos;
- Instalação de firewalls nas LANs de destino das atualizações, a fim de possibilitar o bloqueio de atualizações cruzadas;
- Utilização de política de bloqueio, sem uso de controle de tráfego por serviço. Tal funcionalidade não atende a premissa do serviço de antivírus, que requer que as atualizações sejam imediatamente distribuídas e atualizadas, independente de horário;
- Inserção de mais um ponto de falha na rede; e
- Inserção de mais um dispositivo para administração das equipes de TI.

As atualizações utilizam os seguintes protocolos e portas de comunicação:

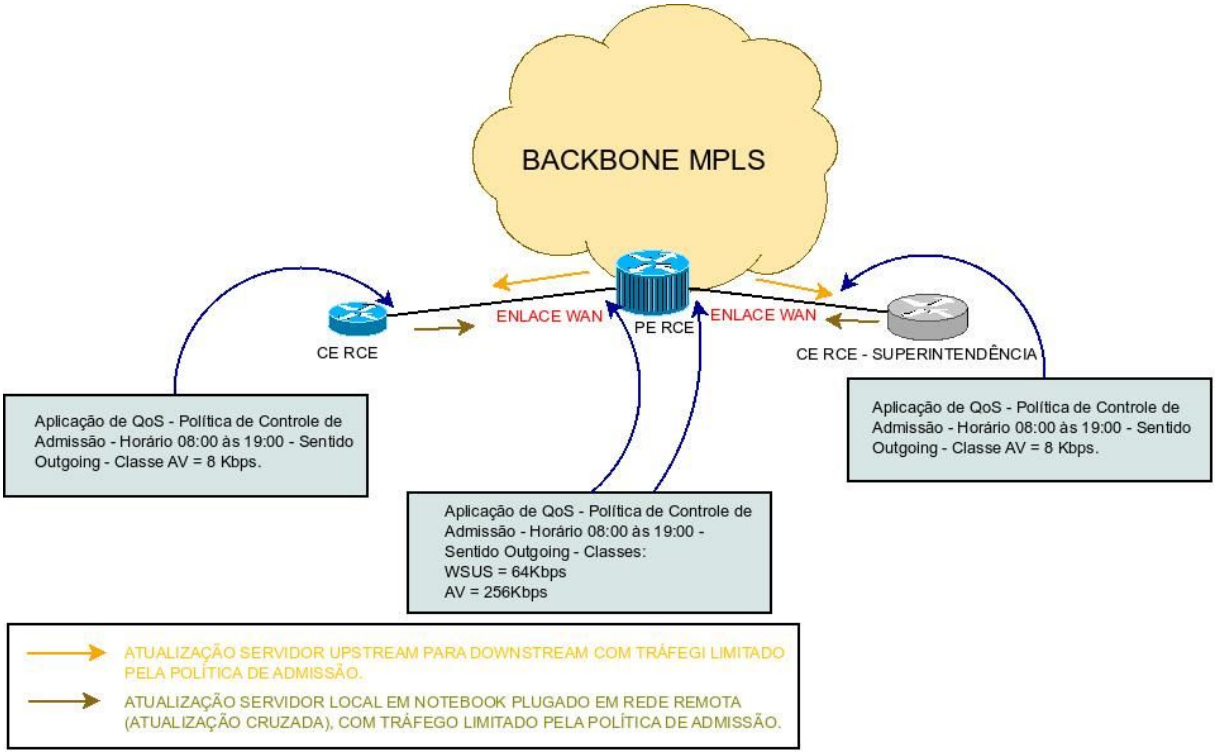
- WSUS: Transport Control Protocol (TCP)/8530
- Antivírus Symantec: TCP/8014 para replicação entre servidores e TCP/2967 para atualizações de estações (Atualização cruzada).

5 SOLUÇÃO

Para a resolução dos problemas apresentados pelos serviços de WSUS e Antivírus, foi adotada a criação de uma política de QoS, baseada no mecanismo de controle de admissão de tráfego. Tal política foi configurada nos equipamentos de

Backbone MPLS do tipo PE (*Provider EDGE),* no sentido *downstream*, e equipamentos de última milha, no sentido *upstream*, instalados nas unidades de rede local do órgão federal, também conhecidos como CE (*Customer EDGE)*. A Figura 4 ilustra a solução.

Figura 4. Configuração de Qos - Política de Admissão.



Fonte: Elaborada pelo autor (2017).

A criação da política de admissão de tráfego consistiu em adicionar ao QoS já existente do órgão, que é baseado no controle de congestionamento CBWFQ (*Class-Based Weighted Fair Queueing)* e LLQ (*Low Latency Queueing*), mais duas classes de tráfego. A WSUS, para *Windows Server Update Service,* e a AV, para Antivírus, ambas associadas a uma política de tempo, onde no período compreendido entre às 8h e 19h, o tráfego de WSUS e Antivírus são limitados a tráfegos preestabelecidos pela política de admissão. Os tráfegos definidos pela política de admissão para WSUS e Antivírus nos PEs foram, respectivamente: 64Kbits/s e 256Kbits/s. Para os CEs, apenas foi necessário realizar o controle no tráfego de AV, limitando a apenas 8Kbits/s, conforme ilustrado na Figura 4.

Cabe salientar que as transmissões fora do intervalo de tempo mencionado, que é configurado na *Access Control List (ACL)* temporal, não sofrem influência da política de admissão de tráfego. Nesta condição, as transmissões de ambos os serviços passam a ser gerenciados pela classe *Best Effort (BE)*.

Como já mencionado, as classes de WSUS e AV são marcadas e classificadas de acordo com uma ACL temporal específica, baseada em critérios e condições. Tais condições é que permitem que o tráfego destes serviços seja detectado e separado das demais classes. Uma vez que o tráfego seja mapeado pela ACL e que todas as condições sejam atendidas, a transmissão dos pacotes se dará de acordo com a política de admissão configurada para cada classe. Os critérios e condições adotados pela ACL temporal das classes de WSUS e AV, são: Protocolo de transporte TCP, origem da transmissão, destino da transmissão, porta de comunicação do serviço e horário em que ocorre a transmissão. Sendo assim, temos:

- ➔ Para WSUS
    - Protocolo: TCP
    - Origem: Qualquer origem
    - Destino: Qualquer destino
    - Porta: 8530
    - *Time-range*: 08:00 às 19:00
- ➔ Para antivírus
    - Protocolo: TCP
    - Origem: Qualquer origem
    - Destino: Qualquer destino
    - Porta: 8014
    - *Time-range*: 08:00 às 19:00

Aliado as configurações de QoS, outras configurações também devem ser realizadas para permitir o correto funcionamento da política de horários estabelecida para os serviços de WSUS e Antivírus. O serviço do *Network Time Protocol (NTP)* é um deles, e é o responsável pelo correto funcionamento do relógio dos roteadores.

Cabe informar que todas as classes de QoS configuradas devem estar associadas a uma *policy*, que por sua vez deve estar associada a interface de rede

que se deseja aplicar o gerenciamento e o controle de filas e tráfego. O sentido do tráfego da interface que a policy deve ser aplicada também deve ser informada. Para o caso dos PEs e CEs, o sentido sempre é de *outgoing*, ou saída da interface.

A ordem em que as classes estão configuradas na *policy* influencia diretamente no funcionamento da política. As classes são verificadas de cima para baixo, da esquerda para a direita. Para que as classes WSUS e AV funcionem de forma apropriada, de acordo com as configurações associadas às classes e as ACLs temporais, é necessário que estejam na parte superior da *policy*. Dessa forma, temos de forma resumida a configuração da *policy* para PE, conforme Tabela 1:

Tabela 1. Policy aplicada para roteadores do tipo PE

CLASSE	POLÍTICA DE ADMISSÃO (Kbps)	PRIORIZAÇÃO DE FILA (% da banda total)	HORÁRIO DE APLICAÇÃO
AV	256	-	08:00 às 19:00
WSUS	64	-	08:00 às 19:00
RT	-	10	o dia todo
VD	-	30	o dia todo
DP	-	10	o dia todo
DC	-	30	o dia todo
BE	-	20	o dia todo

Fonte: Elaborada pelo autor (2017).

Assim como nos equipamentos do tipo PE, a política de admissão também é necessária nos CEs para solucionar o problema da atualização cruzada do serviço de antivírus, como já mencionado anteriormente. As configurações praticamente são as mesmas, mas se diferenciam com relação ao PE nos seguintes quesitos:

1. Necessidade de configuração apenas da classe AV. O serviço de WSUS não ocasiona atualização cruzada.
2. Política de admissão da classe AV com limitação de tráfego em até 8Kbps.
3. Ajuste da porta de transmissão do serviço para TCP 2967.

4. Configuração da policy para CE, conforme Tabela 2.

Tabela 2. Policy aplicada para roteadores do tipo PE

CLASSE	POLÍTICA DE ADMISSÃO (Kbps)	PRIORIZAÇÃO DE FILA (% da banda total)	HORÁRIO DE APLICAÇÃO
RT	-	10	o dia todo
AV	8	10	08:00 às 19:00
VD	-	30	o dia todo
DP	-	10	o dia todo
DC	-	30	o dia todo
BE	-	20	o dia todo

Fonte: Elaborada pelo autor (2017).

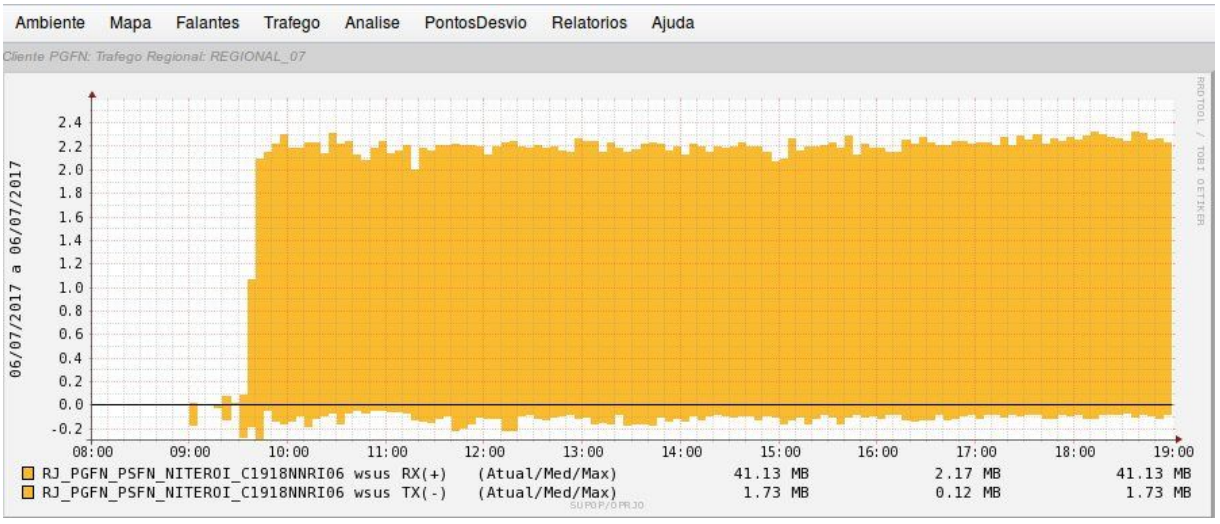
Os equipamentos utilizados são da Cisco e, portanto, toda a sintaxe de comandos obedece o padrão estabelecido pela plataforma IOS do sistema operacional deste fabricante. As configurações dos equipamentos podem ser vistas no Apêndice A deste documento.

6 CONCLUSÃO

As configurações de controle de admissão criadas para os serviços de WSUS e antivírus conseguiram controlar os tráfegos de atualização, conforme as políticas de tráfego e de tempo configuradas. Os resultados e a aferição da configuração pôde ser medida através de monitoração, utilizando um recurso de gerenciamento especialmente desenvolvido para este fim. O desenvolvimento de tal ferramenta consistiu em extrair dos PEs e CEs, através de *NETFLOW*, fluxos de rede dos enlaces WAN monitorados, para a partir disso, e de acordo com as portas de transmissão TCP 8014, 8530 e 2967, criar um banco de dados de tráfego dos serviços de WSUS e antivírus. A ferramenta então realiza a cada 10 minutos a avaliação de tráfego dos últimos 30 minutos de dados inseridos no banco de dados, no horário compreendido entre às 08:00 e 19:00. Caso a soma total do fluxo de transmissão de dados dos últimos 30 minutos exceda o valor de 13MB, a ferramenta irá alarmar através de um *trap* desvio na política de admissão e, por consequência,

elevada transmissão na atualização dos serviços em horário comercial. Caso o tráfego esteja dentre o limite definido, a ferramenta não tomará nenhuma ação, apenas plotando o gráfico de transmissão do serviço, validando assim que a política de admissão está funcionando de forma correta. As Figuras 5 e 6 abaixo ilustram a plotagem de tráfego da ferramenta de gerência, indicando o correto funcionamento da política de admissão para WSUS.

Figura 5. Política de admissão de tráfego do enlace da localidade A em funcionamento, no horário das 08:00 às 19:00. Tráfego linear, limitado a média de transmissão total de 2.17MB, medido no intervalo de 5 minutos.



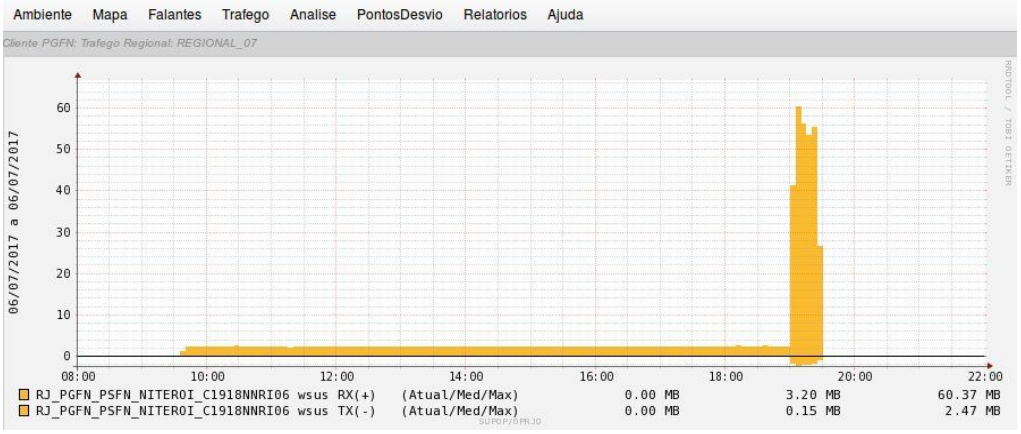
Fonte: Plataforma de gerenciamento de rede e gestão de desempenho do Serviço Federal de Processamento de Dados. (2017).

Se o volume de dados transmitidos de 2.17MB em 5 minutos for convertido para a taxa de transmissão de rede medida em Kilobits por segundo (Kbps), veremos que a política de admissão configurada para a classe de WSUS está funcionando de acordo com a taxa de 64Kbits/s aplicada a classe. Sendo assim, temos o seguinte cálculo:

1. Converter 2.17 MB em Mbits: 2.17 x 1024 = 2222.08 KBytes
2. Converter 2222.08 KBytes em Kbits: 2222.08 x 8 = 17776.64 Kbits
3. Converter 17776.64 Kbits medidos 5min para a taxa em 1 segundo: Se 5 min = 300 segundos, então 17776.64/300 = 59.25 Kbits/s.

A taxa de 59.25 Kbits/s se aproxima bastante da taxa de admissão de tráfego de 64Kbits/s configurada para a classe de WSUS. A precisão não deve ser considerada devido aos cabeçalhos de transmissão e a cálculos matemáticos inerentes a ferramenta de gerência. O gráfico se mantém linear, sem crescimento, indicando o funcionamento da política de admissão imposta, que limita o tráfego a taxa de 64Kbits/s.

Figura 6. Funcionamento da política de admissão de tráfego do enlace de rede da localidade A no horário das 08:00 às 22:00. A partir das 19:00 a transmissão pode ocorrer até o limite máximo do circuito. A transmissão máxima da atualização a partir das 19:00 atingiu 60.37MB.



Fonte: Plataforma de gerenciamento de rede e gestão de desempenho do Serviço Federal de Processamento de Dados. (2017).

O relatório técnico demonstra que mesmo que as ferramentas e/ou serviços de atualização sejam capazes de trabalhar com agendamento, é possível que falhas ocorram, fazendo com que as atualizações possam ocorrer dentro de horários em que existem concorrência de tráfego com outros serviços. A política de admissão de QoS, associada à lista de acesso temporal, adiciona uma proteção a mais para que os serviços de atualização, independentemente de erros ou falhas, não impactem no tráfego de serviços mais prioritários dos usuários, não deixando também de realizar suas funções, também tão importantes para a segurança, inovação de recursos e disponibilidade da rede.

.

REFERÊNCIAS BIBLIOGRÁFICAS

Microsoft. Sobre o WSUS. Disponível em: <https://msdn.microsoft.com/pt-br/library/hh852345(v=ws.11).aspx>. Acesso em 29 de Maio de 2017.

Implementing Cisco Quality of Sevices (QoS): Student Guide. Versão 2.0. USA: knowledgenet, 2004. 1067 p.

Odom, Wendell; Cavanaugh, Michael J.. Cisco QoS Exam Certification Guide: IP Telephony Self-Study. 2ª Edição. Indianapolis, USA: Cisco Press, 2005. 764 p.

Tanenbaum, Andrew S.; Tradução Vandenberg D. de Souza. Redes de Computadores. 4ª Edição. Rio de Janeiro, BRA: Elsevier, 2003. 1944 p.

Odom, Wendell. Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide. 1ª Edição. Indianapolis, USA: Cisco Press, 2013. 899 p.

APÊNDICE A - Comandos Aplicados nos Roteadores

1 COMANDOS A SEREM APLICADOS EM ROTEADORES PE

1.1 CRIAÇÃO DAS CLASSES

Inicialmente devem ser criadas as classes no roteador, para em seguida serem vinculadas às políticas. Cada classe utiliza uma maneira específica para classificar o tráfego desejado. Abaixo estão os comandos necessário e a explicação de cada um:

- Classe do Antivírus, utiliza ACL

```
class-map match-any AV/TC-PE
match access-group name ACL_AV
```

- Classe do WSUS, utiliza ACL

```
class-map match-any WSUS/TC-PE
match access-group name ACL_WSUS
```

- Classe Real Time, para áudio, utiliza DSCP

```
class-map match-any RT/TC-PE
match ip dscp ef
```

- Classe Vídeo, utiliza DSCP

```
class-map match-any VD/TC-PE
match ip dscp af41
```

- Classe Dados Prioritários, utiliza DSCP

```
class-map match-any DP/TC-PE
match ip dscp af31
match ip dscp af11
```

- Classe Dados Corporativos, utiliza DSCP

```
class-map match-any DC/TC-PE
match ip dscp af21
match ip dscp af12
```

- Classe Best Effort, utiliza DSCP e o que não estiver marcado

```
class-map match-any BE/TC-PE
match ip dscp default
match ip dscp af13
```

1.2 CRIAÇÃO DAS POLÍTICAS

Com as classes criadas, o próximo passo é criar as políticas que dirão ao roteador como tratar o tráfego de cada classe:

- Política principal, utilizando shape para WSUS e SEP, bandwidth para as demais e random-detect para atenuar picos e timeouts, e queue-limit também para evitar timeout.

```
Policy-map TC-PE/1006-GE/OUT/V1:ORGAO_VCD
class AV/TC-PE
shape average 256000
class WSUS/TC-PE
shape average 64000
class RT/TC-PE
priority percent 10
class VD/TC-PE
bandwidth percent 30
class DP/TC-PE
bandwidth percent 10
random-detect dscp-based
random-detect dscp 26 30 ms 100 ms 10
queue-limit 200 ms
class DC/TC-PE
```

```
bandwidth percent 30
random-detect dscp-based
random-detect dscp 18 30 ms 100 ms 10
queue-limit 200 ms
class BE/TC-PE
bandwidth percent 19
random-detect dscp-based
random-detect dscp 0 30 ms 100 ms 10
queue-limit 200 ms
```

Obs.: caso já exista uma Policy com o mesmo nome criada no roteador PE será necessário removê-la antes de incluir os comandos acima, para que a ordem das classes seja mantida conforme documento.

- Política encadeada, necessária quando o roteador não permite aplicar a política principal diretamente na interface. Ex. Conexão Ethernet que precise de configurações de limitação de banda além do QoS.

```
policy-map TC-PE/OUT/V1:ORGAO_VCD/XM
class class-default
shape average bandwidth_circuito bandwidth_circuito/100 0
service-policy TC-PE/OUT/V1:ORGAO_VCD
```

Abaixo um exemplo da configuração de política, em um caso onde a policy foi criada em um roteador PE Cisco ASR-1006X, aplicada numa interface GigabitEthernet e específica para um circuito de 4Mbps:

```
policy-map TC-PE/OUT/V1:ORGAO_VCD/4M
class class-default
shape average 4096000
service-policy TC-PE/OUT/V1:ORGAO_VCD
```

```
interface GigabitEthernet0/1/4.2010
description PSFN XYZ
bandwidth 4096
encapsulation dot1Q 2010
service-policy output TC-PE/OUT/V1:ORGAO_VCD/4M
```

1.3 CONFIGURAÇÕES PARA WSUS E ANTIVÍRUS

Para que ocorra a limitação do tráfego do WSUS e do Antivírus, é necessário criar listas de acesso e criar uma faixa de tempo, de forma a categorizar e limitar o tráfego somente no horário comercial, permitindo assim o livre funcionamento das atualizações durante a noite.

- Configuração do período comercial

```
time-range WSUS-AV-ORGAO
periodic weekdays 8:00 to 19:00
```

- Configuração das listas de acesso

```
ip access-list extended ACL_AV
remark porta tcp 8014 ANTIVIRUS
permit tcp any any eq 8014 time-range WSUS-AV-ORGAO
permit tcp any eq 8014 any time-range WSUS-AV-ORGAO
ip access-list extended ACL_WSUS
remark porta tcp 8530 WSUS
permit tcp any eq 8530 any time-range WSUS-AV-ORGAO
permit tcp any any eq 8530 time-range WSUS-AV-ORGAO
```

2 COMANDOS A SEREM APLICADOS EM ROTEADORES CE

Para os equipamentos do tipo CE, instalados nos clientes é necessário que também categorizemos os dados, separando assim o tráfego dos codecs, da voz, dos sistemas prioritários do resto do tráfego com menor prioridade. Essa seção contém os blocos de configuração necessários para tal configuração em diversas

marcas e tecnologias hoje presentes no parque tecnológico do SERPRO e do cliente.

2.1 CRIAÇÃO DOS ROUTE-MAPS E LISTAS DE ACESSO

```
ip access-list extended ACL_SUPORTE
permit udp any any eq snmp
permit udp any eq snmp any
permit udp any any eq snmptrap
permit udp any eq snmptrap any
permit tcp any any eq telnet
permit tcp any eq telnet any
permit udp any any eq tftp
permit udp any eq tftp any
permit tcp any any eq 22
permit tcp any eq 22 any
permit udp any any eq ntp
permit udp any eq ntp any
permit tcp any any eq tacacs
permit tcp any eq tacacs any
permit udp any any range 1645 1646
permit udp any range 1645 1646 any
permit udp any any range 1812 1813
permit udp any range 1812 1813 any

ip access-list extended ACL_CODEC
permit ip host ip_codec any

ip access-list extended ACL_DC
remark Redes Intranet e Sistemas/Servicos Internet hospedados no SERPRO
permit ip any 10.0.0.0 0.255.255.255
permit ip any 172.16.0.0 0.15.255.255
```

```
permit ip any 192.168.0.0 0.0.255.255
permit ip any 161.148.0.0 0.0.255.255
permit ip any 189.9.0.0 0.0.255.255
permit ip any 200.198.192.0 0.0.63.255

ip access-list extended ACL_BE
permit ip any any

ip access-list extended ACL_AV
remark porta tcp 2967 ANTIVIRUS – BLOQUEIA ATUALIZACAO CRUZADA
permit tcp any any eq 2967 time-range WSUS-AV-ORGAO
permit tcp any eq 2967 any time-range WSUS-AV-ORGAO

route-map INTERNO permit 10
match ip address ACL_SUPORTE
set ip precedence immediate
set ip tos max-throughput
route-map INTERNO deny 20

ip local policy route-map INTERNO
```

- Configuração do Time Range (período comercial)

```
time-range WSUS-AV-ORGAO
periodic weekdays 8:00 to 19:00
```

2.2 CRIAÇÃO DAS CLASSES

```
class-map match-all RT/TC-CE
match access-group name ACL_CODEC
match ip dscp 46
```

```
class-map match-any AV/TC-CE
match access-group name ACL_AV
class-map match-all VD/TC-CE
match access-group name ACL_CODEC
match ip dscp 34

class-map match-any DP/TC-CE
match access-group name ACL_CODEC
match ip dscp 26
match ip dscp 10

class-map match-any DC/TC-CE
match access-group name ACL_DC
match ip dscp 18
match ip dscp 12

class-map match-any BE/TC-CE
match access-group name ACL_BE
```

2.3 CRIAÇÃO DAS POLÍTICAS

```
policy-map TC-CE/IN
class RT/TC-CE
police rate percent 10 burst 1000 ms
conform-action set-dscp-transmit ef
exceed-action drop
priority percent 10
class AV/TC-CE
police 8000
class VD/TC-CE
police rate percent 30 burst 1000 ms
conform-action set-dscp-transmit af41
exceed-action drop
```

```
bandwidth percent 30
class DP/TC-CE
police rate percent 10 burst 1000 ms
conform-action set-dscp-transmit af31
exceed-action set-dscp-transmit af11
bandwidth percent 10
class DC/TC-CE
police rate percent 30 burst 1000 ms
conform-action set-dscp-transmit af21
exceed-action set-dscp-transmit af12
bandwidth percent 30
class BE/TC-CE
police rate percent 20 burst 1000 ms
conform-action set-dscp-transmit default
exceed-action set-dscp-transmit af13
bandwidth percent 20
```

Obs.: caso o roteador mostre mensagem informando não ser possível alocar a porcentagem de 20% para a classe BE/TC-CE, deve-se alterar o valor para **19**.

2.4 CONFIGURAÇÃO DAS INTERFACES

Após haver preparado toda a configuração, categorização, priorização, filtros e limitações, deve-se aplicar a política a uma interface para que o tráfego transmitido/recebido por esta seja processado e corretamente classificado.

- Interface Ethernet:

```
interface FastEthernetX/Y ou GigabitEthernetX/Y ou Vlan X
description Circuito ORGAO x PE Serpro
ip route-cache policy
load-interval 30
max-reserved-bandwidth 100
service-policy output TC-CE/IN
```

- Interface ATM:

```
interface ATMX/Y
description Circuito RFB x PE Serpro
ip nbar protocol-discovery
ip route-cache policy
load-interval 30
pvc X/Y
service-policy output TC-CE/IN
```

- Interface Serial:

```
map-class frame-relay TC-CE/Banda_Circuito
frame-relay cir Banda_Circuito
frame-relay bc Banda_Circuito/100
frame-relay be 0
frame-relay mincir Banda_Circuito
service-policy output TC-CE/IN
interface SerialX/Y/Z
load-interval 30
no fair-queue
frame-relay traffic-shaping
interface SerialX/Y/Z.x point-to-point
ip nbar protocol-discovery
frame-relay class TC-CE/Banda_Circuito
```

Exemplo para circuito Frame-Relay de 2Mbps

```
map-class frame-relay TC-CE/2M
frame-relay cir 2048000
frame-relay bc 20480
frame-relay be 0
frame-relay mincir 2048000
service-policy output TC-CE/IN
```