XCA EDGE Use case
MIXED IPSEC / MPLS-VPN
NETWORK OPTIMIZATION
About this document

This document introduces a general use case of the Expereo XCA Edge solution. As it deals with a linear and chronological example, it is a perfect tool to understand the underlying concepts of our product. It will also help you if you need an overview of all the benefits you could get from XCA Edge.

Note that this use case only covers one of the several usages of XCA Edge. However, there is a good chance that a large part of this use case applies to your own configuration. If not, please have a look to the other use cases.

Moreover, if you need more specific information, please refer to the XCA Edge Administrator Manual. It contains a more precise description of the XCA Edge features, and provides per-page explanations of the graphical user interface.

Abstract

BarSolutions is a worldwide extended company that has built its network over a combination of IPSec tunnels and MPLS-VPN networks. It set up a star-based topology, where the routing between the several available paths is done thanks to the BGP protocol.

From the main data center, BarSolutions would like to use XCA Edge to achieve specific goals:

• Balance the load between the several available paths to reach distant sites,
• Prioritize critical subnets (VoIP),
• Monitor the link quality to distant sites and raise alarms when needed,
• Have a complete report on each available path usage.

<table>
<thead>
<tr>
<th>Situation</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to evaluate the per IPSec tunnel / per MPLS-VPN connection usage.</td>
<td>Use the transits related reporting tools to evaluate how is the traffic divided into the several available paths.</td>
</tr>
<tr>
<td>Lack of information on traffic per destination prefix (to evaluate required network access bandwidth).</td>
<td>Use the destinations related reporting tools to evaluate the per-destination traffic.</td>
</tr>
<tr>
<td>Need to optimize bandwidth usage or reduce RTD.</td>
<td>Select a routing policy, and enable the routing optimization.</td>
</tr>
<tr>
<td>Need to prioritize specific destinations.</td>
<td>Insert a static routing order into XCA Edge.</td>
</tr>
</tbody>
</table>
1. Introduction

1.1. Introduction

BarSolutions is a worldwide extended company, divided in hundreds of entities over the world. To connect its sites, BarSolutions set up an architecture based on a combination of MPLS-VPN virtual networks and IPSec tunnels.

Its main data center is connected to two MPLS-VPN networks provided by two different ISP: Fastcomz and Speedcomz. These MPLS-VPN networks are managed by a single Service Provider, end-to-end. They offer guaranteed levels of services. IPSec tunnels go through the Internet. Hence, they are dedicated to applications that can cope with best effort handling.

The company evaluated several criticality levels concerning its distant sites, and chose its connectivity accordingly:

- Highly critical sites are connected through both Fastcomz and Speedcomz MPLS-VPN networks,
- Critical sites are connected to at least one MPLS-VPN network, and use a IPSec tunnel as a support/backup to the data center,
- Less critical sites are connected to the data center through a single IPSec tunnel.

![Figure 1: BarSolutions network architecture](image-url)
Within each site, the IP addressing is divided into subnets according to the needed quality of service (QoS). As an example, multiples sites use a VoIP (Voice over IP) service: IP phones are directly included in specific subnets that, whenever possible, must be routed through the MPLS-VPN network. Therefore this traffic will benefit from the appropriate level of QoS prioritization and related SLAs.

Note that this design is based on the network layer, hence this type of prioritization only gives each device a single level of QoS. So far, we can divide applications into the following sets:

- Internet access: routed through local breakout,
- Critical applications - VoIP (Voice over IP), security (fire detection, alarms, access badges), funds flows: routed through the MPLS-VPN network,
- Best effort - everything else: routed through the IPSec tunnel.

Note: In many architecture, the best effort traffic becomes more and more important, as numerous services are now web-based (phone/video calls, webservices...).

As sites are numerous, BarSolutions decided to use the BGP protocol to route traffic within its own networks. Each site has a single AS number but may include several subnets.

BarSolutions has set up its XCA Edge server within the main data center.
2. Use case steps

2.1. Step 1: Route VoIP on MPLS-VPN networks for critical destinations

As shown on Figure 1, critical destinations have connectivity to both a VPN tunnel and a MPLS-VPN network. As VoIP traffic must be considered as high-priority traffic, it has to be routed, whenever possible, through the MPLS-VPN network. Consequently, low priority subnets should be routed through the IPSec tunnel.

To achieve this goal, the network administrator has to execute two operations:

- Insert a static routing order within the data center router (for outgoing traffic),
- Configure the routers to announce a prepended AS-path towards critical subnets on the IPSec link (for incoming traffic).

Figure 2 illustrates these operations. Note that a single router in used here, but this also applies when several routers are used (one for each path).

2.1.1. Static routing configuration

Outgoing traffic that has a destination address towards a remote VoIP subnet needs to be routed through the MPLS-VPN network (when available). Therefore, the network administrator wants to manually set the route for these subnets. He accesses the Routing / Engine menu, and clicks on the "Managed subnets" tab.

He first searches for one of the VoIP remote subnets using the top search field. When he finds it, he edits the corresponding line by clicking on the pen icon on the right.
By selecting the right transit in the "Static routing" drop-down list, the network administrator generates and executes an automatic routing order. This routing order will not be modified by the Routing Decision Engine.

However, because the MPLS-VPN network could face failures, XCA Edge implement a static route failover mechanism. Within the RDE Settings tab, the network administrator can configure when a statically routed traffic might be rerouted. Both loss ratio and RTD limits shall be set. In version 1.1, this is a global setting for all subnets.

**2.1.2. Static AS-prepending configuration**

To statically route the incoming traffic, the network administrator must configure the IPSec link AS-path prepending. This will make its routers suggest to the distant sites that the IPSec link is longer than the MPLS-VPN, when they want to reach a critical subnet.

Note that the per-subnet incoming traffic rerouting is not provided by XCA Edge itself, but by the routers. XCA Edge can only operate a per-transit routing optimization concerning incoming traffic (see step 3). This might be subject to change in a further version.
2.2. Step 2: Outgoing traffic routing optimization

To optimize routing toward remote subnets, XCA Edge relies on automatically or manually created probes. The Routing Decision Engine, according to the configured routing policy, selects the best route available and generates pertinent routing orders. Each routing policy might optimize speed, cost, or any other metrics. Expereo provided BarSolutions with a routing policy fitting its needs.

The network administrator would like to optimize the routing towards the critical destinations subnets (connected to both MPLS-VPN networks). To optimize the outbound routing, the network administrator first need to configure the probing engine. He chooses to use manual probes, as he knows specific destinations within each remote subnets (file servers, routers ...) that will always be reachable.

The "Optimized IPSec WAN" use case explains how these manual probes can be created, please refer to this document for more information.

Within the Routing / Engine - RDE settings panel, the network administrator can select the routing policy. He select the proper routing policy: Cost control. This routing policy will make traffic use the best transit available until it reaches the CDR.

Once the routing policy is selected, the network administrator can choose the RDE operation mode. In the “Outgoing optimizations” drop-down list, three modes are available:

- Disabled: no routing optimization is performed,
- Semi-automatic: routing orders are generated, but must be manually executed. This should be used for routing policy testing.
- Automatic: the network administrator chooses this mode. It automatically executes the generated routing orders.

Once the configuration is saved, the RDE will start generating orders and optimize outbound routing whenever this is possible.
2.3. Step 3: Incoming traffic routing optimization

Although BGP limitations prevent XCA Edge from forcing incoming traffic to use a specific transit, it is able to suggest remote subnets a best route. The AS-prepending feature makes BGP routers announce that specific paths are longer than they actually are.

Note: Unlike the per-subnet rerouting mentioned in step 1, the XCA Edge incoming traffic optimization will influence all incoming traffic. This provides a per-transit granularity in traffic optimization.

AS-prepending script configuration

To optimizes incoming traffic, the network administrator needs to configure the script that will be used to prepend the AS-path on chosen transits. He accesses the Network / BGP routers menu, and edit involved routers.

At the bottom of the page, he can configure the script used to prepend an AS-path, provided that the SSH access is configured.
Inbound script identifier configuration

From the Network / Transit menu, the network administrator edits the corresponding transits. He chooses distinctive identifiers for each transit. This will be used by the AS-prepending script.

RDE inbound optimization activation

Once AS-prepending is configured, the network administrator can activate the inbound routing optimization. He accesses the Routing / Engine menu and go to the
“RDE settings” tab. On the top on the page, he sets the Inbound optimization as "Automated".

According to the routing policy configured within this page, the Routing Decision Engine will automatically generate and execute routing orders. The routing policy applies the same algorithm for inbound or outbound optimization. Therefore, the incoming traffic will be routed through the best transit until it reaches the CDR.

2.4. Step 3: Distant subnet monitoring

Thanks to XCA Edge, the network administrator is able to monitor remote subnets availability. Within the Prefix section, he can access monitoring tools and configure alarms for specific events. The network administrator can configure the monitoring engine so that, whenever an alarm raises, it sends an email or an SMS. The GUI might also display several alarms through the Notification / List section.

In BarSolutions architecture, AS-paths to VoIP subnets should have fixed length. Whenever the AS-path length increases, this means that the path from the source to the destination has changed. As an example, if the AS-path towards a critical destination’s VoIP subnet increases, this means that the corresponding traffic is now routed through the IPSec tunnel.

Therefore, the network administrator configured an alarm for this event (Figure 7). Please refer to the "Optimized IP WAN" use case for more details on the monitoring engine configuration.

![Figure 7: We raise an alarm when the AS-path length increases](image)

Also to have a better view of the network status, a map is also available in the Geolocation / Map section (Figure 8).
2.5. Step 4: Per-subnet reporting, bandwidth usage.

XCA Edge provides the network administrator with a set of reporting tools that can help him to understand its current situation. Thus, he will be able to evaluate which transits or peerings are the most important to BarSolutions business.

These tools help him to decide whether or not he needs to establish new peerings, connect to new transits or improve currently contracted CDRs. Note that the "Basic reporting" use case deals with these reporting tools. Please read it for further information.

Evaluating, for each destination, the routing performances.

By accessing the Prefix / Summary section (Figure 9), the network administrator can evaluate if a subnet is properly routed. He searches, using the top field, the VoIP subnets he wanted to be correctly routed. As configured, the report shows that the VoIP subnets are routed through the MPLS-VPN transit.

Whenever a subnet traffic (inbound or outbound) uses multiple transits, a deeper analysis can be performed using the Traffic / Destination - History report. This report shows the per-transit distribution of a subnet traffic over time. This is useful to understand how your configured routing policy influences the routing.
Transit usage, load balancing

XCA Edge is able to generate smart reports from the data collected by the traffic engine. Within the Traffic menu entry, several reporting pages are available. Reporting tools can be used to:

- Evaluate, for each destination, which transits are used,
- Evaluate which destinations generate the most important traffic,
- Evaluate each transit load, aggregated or over time,

Concerning its own architecture, the network administrator can, as an example, have a look to the Traffic / Transit - History page. Figure 10 illustrates the per-transit bandwidth usage over time. As we can see, the routing optimization engine has been able to reroute the traffic wherever an overload occurs.
Figure 10: Transit usage over time
3. Conclusion

XCA Edge provides BarSolutions with a plug & play optimization of performance, availability and bandwidth resources. The network administrator has now a better view on the actual effective routing. He is able to provide BarSolutions collaborators with the best possible service within the actual network infrastructure.

Also, XCA Edge monitoring tools gives him the ability to be as reactive as possible whenever a network failure occurs.