

# VPN Resiliency

IPSec VPNs are designed to provide secure connectivity, but how effective is the solution if the connectivity is not available when enterprises need it? Juniper Networks offers the first IPSec VPN solution capable of providing system-level resiliency for a truly fault tolerant solution that will meet an enterprise’s connectivity needs. As a result, many of Juniper’s customers have said that their network connectivity and reliability is the best it has ever been after deploying the Juniper Networks dynamic VPNs. With Juniper’s VPNs, enterprises can:

- Reduce reliance on a single transport mechanism or service provider with physical path redundancy
- Reduce the possibility of a single point of failure with redundant devices and redundant components in those devices, with state sync and VPN sync
- Reduce the reliance on manual intervention to establish a new route with dynamic routing
- Reduce the failover time of a VPN connection with redundant VPN tunnels and VPN monitoring

Juniper’s security solutions are enablers of connectivity, providing a resilient solution that includes Stateful high availability capable of sub-second failover. With the Juniper Networks VPN solution, enterprises can be confident that their VPN is going to give them the secure, “always on” connectivity that they need, so they can concentrate on the projects that are core to their business success.

While other solutions offer bits and pieces, Juniper Networks is the first to put it all together for system-level resiliency.

<b>VPN session</b>	<b>Redundant VPN gateways, Security Association mirroring, VPN path monitoring, route based VPN</b>	} Only when considered together can complete resiliency be achieved
<b>VPN Components</b>	<b>NetScreen VPN resiliency features</b>	
<b>Session</b>	<b>Stateful fail-over</b>	
<b>Device</b>	<b>Redundant gateway. Redundant components (Power Supply, fans, etc.)</b>	
<b>Logical path</b>	<b>Dynamic routing</b>	
<b>Physical path</b>	<b>Redundant path</b>	

## Redundant Paths

If the physical connection goes down, the VPN goes down. To improve resiliency, Juniper’s VPN solution supports multiple physical paths. As a result, Juniper Networks gives enterprises the flexibility to determine the alternate transport options, based on the cost and resiliency requirements.

There are any number of possible configurations enterprises can deploy. For example, in a remote office with less than 50 people, the cost of the alternative transport is probably a large factor. While it’s probably not affordable to wait for someone to physically reestablish a connection, organizations could live with 1-2 minutes of down time. As a result, on-demand failover from a dial backup might be the option for alternate transport.

The branch office, on the other hand, probably requires a higher degree of failover resiliency, so organizations might choose a dedicated DSL. The important thing is that the use of parallel physical paths between two sites reduces the dependency on any one mode of transport or network provider and offers persistent connectivity during path failure.

Juniper Networks enables enterprises and service providers to choose the parallel paths that meet the requirements for each and every segment of the network.

Some vendors cannot support dynamic routing in their product, so they leverage the dynamic routing protocol of the service providers. Unfortunately, service providers want to limit the size of their dynamic routing tables, so they only allow the use of BGP, which stands for Border Gateway Protocol, for customers that have large networks (usually more than 4000 contiguous IP addresses). BGP is the dynamic routing protocol that enables the same network to connect to different service providers. As a result, branch offices and many corporate offices are unable to use BGP to support redundant paths. As a result, an alternate mechanism is required.

Because Juniper's VPNs support dynamic routing, as well as multiple VPN tunnels, we can solve this problem. Enterprises can build a VPN tunnel to each ISP provider and then run OSPF, which stands for Open Shortest Path First, a different dynamic routing protocol that doesn't have the restrictions of BGP, over the tunnels. OSPF will identify when a tunnel goes down and switch to the other one. However, the latency of this switch over can be up to a minute, because OSPF relies on "broadcasts" to learn that a device or connection went down.

Juniper Networks can also give organizations a solution that can achieve failover latency of a few seconds. Using Juniper's unique VPN monitoring can be used to constantly monitor the tunnels and instantaneously switch over in the event of a failure.

NOTE: Redundant Paths support requires dynamic routing

### **Dynamic Routing**

Juniper Networks' purpose-built security solutions were designed to fit seamlessly into any network. The ability to be part of any routing infrastructure enables Juniper to leverage dynamic routing to simplify deployment and ongoing management of the VPNs and deliver integrated resiliency features in Juniper's integrated firewall and IPSec VPN products. Dynamic routing enables the automatic reroute around trouble spots, including failed or congested links or devices, without the need for manual intervention. It enables many of the features, including dynamic VPNs, path redundancy and full-mesh high availability.

What makes this possible is that all of the routers are continually talking to each other using a broadcast mechanism to "advertise" the routes, so that a communication path can be dynamically maintained. If a connection or route goes down for some reason, the routers will learn that the particular route is no longer available and will look for an alternate path to allow the two end points to talk to each other.

As it relates to VPNs, dynamic routing enables the Juniper Networks solutions to survive failures at the physical layer, so that the VPN tunnel can persist. When dynamic routing determines that there is a failure, Juniper's dynamic VPNs can reroute around that failure to maintain the connection. Because the Juniper security devices are network aware, the device can make "best path" forwarding decisions for individual traffic flows. So, once a connection is back up, Juniper's VPNs will learn about it and automatically start using it again, if it is the best path. As a result, Juniper's dynamic VPNs offer enterprises a resilient solution that doesn't need manual intervention.

It's important to note that dynamic routing protocols, such as Border Gateway Protocol(BGP) and Open Shortest Path First(OSPF), can actually take up to a minute to identify a failure, due to the reliance on the route "broadcasts." As a result, Juniper Networks has taken additional measures, such as VPN monitoring, to create solutions that provide failover in a few seconds.

## VPN Synchronization

It is important that devices in a high availability configuration share the information on the VPN state of the connection. Many security vendors say that they offer Stateful HA. This means that they are able to track the state of the communication, so that a session is not lost if a device fails. It would be a logical extension that the device can also keep the VPN connection going without disruption. Unfortunately, this is NOT the case. Organizations need to make sure that the vendor is capable of also maintaining and sharing the state of the VPN. If the devices don't, when a failure occurs, the security association between the connection and the VPN is lost and needs to be reestablished. This can take 30 seconds to a minute, while the gateways share the keys to re-establish the VPN. This might not be a big deal if there is only one or two VPN connections, but if there are tens, hundreds, or even thousands of VPN connections the down time can be significant. If the devices are sharing both state and VPN information that time is less than a second. Organizations need to make sure that their solution maintains VPN state information to reduce the latency of a device failure.

## VPN Tunnel Redundancy

While enterprises want path redundancy at the physical level to recover from a connection failure, they also want redundancy at the logical VPN layer, so they don't need to wait to establish an alternate VPN path and can minimize that down time. Juniper Networks IPSec VPN solutions support multiple VPN tunnels that mirror the VPN's security associations, so that it can automatically be associated with the live tunnel. However, Juniper's VPNs take it a step further, providing VPN failover in a few seconds. Most solutions, if they offer tunnel redundancy, rely on dynamic routing to learn that one of the tunnels is down before failing over to the other one. The dynamic routing protocols most often used are BGP and OSPF, which can take up to a minute to learn about the failure. Juniper Networks, however, doesn't need to rely on dynamic routing. Instead, Juniper's VPNs use a unique technology, called VPN monitoring, to constantly monitor the tunnels, so that a tunnel failure is rapidly identified and failover can be accomplished in a few seconds. Juniper Networks VPNs can also make "best path" forwarding decisions, looking for the shortest, most direct route, so as soon as the preferred tunnel comes back up, the device will automatically switch back to that route.

