8 Reasons To Go Tunnel-Free

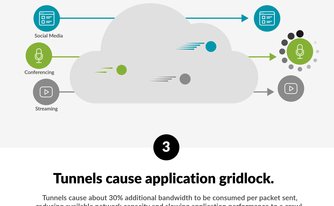
By adding complexity, fragility, expense, and inefficiency, tunneling protocols like IPsec undermine network expressways and cause application performance to break down.

Here's how.

1

Tunnels are a one-lane highway.

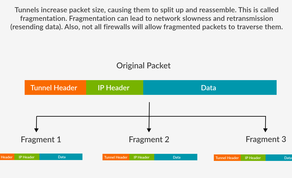
Tunnels look like a singular network flow to routers, with performance that's tied to a single path for long periods. That means there's no way to route to better pathways when congestion strikes.



2

Tunnels punish the non-speeders.

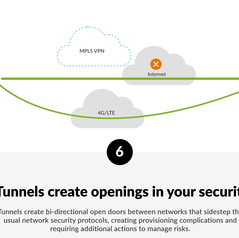
To regulate bandwidth-intensive applications, routers drop packets. But when traffic for multiple applications flows through one tunnel, the network tends to slow down the wrong sessions.



3

Tunnels cause application gridlock.

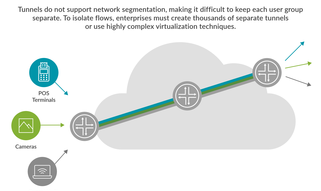
Tunnels cause about 30% additional bandwidth to be consumed per packet sent, reducing available network capacity and slowing application performance to a crawl.



4

Tunnels cause fragmentation.

Tunnels increase packet size, causing them to split up and reassemble. This is called fragmentation. Fragmentation can lead to network slowness and retransmission (resending data). Also, not all firewalls will allow fragmented packets to traverse them.



Reassembly is inefficient on routers

Slows down network traffic

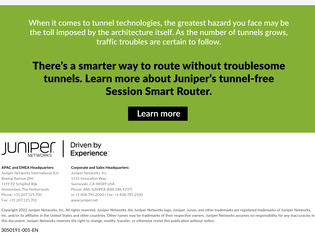
Causes retransmission

Not accepted by all firewalls

5

Tunnels lead to long setup times and delays.

Long tunnel setup times and slow negotiation for security keys create serious delays after failovers that can cause internal applications to reset.



6

Tunnels create openings in your security.

Tunnels create bi-directional open doors between networks that sidestep the usual network security protocols, creating provisioning complications and requiring additional actions to manage risks.

Tunnels bypass network security and filtering

This increases exposure due to NAT holes and public tunnels

This leads to the profiling and targeting of tunnel addresses

7

Tunnels don't segment traffic.

Tunnels do not support network segmentation, making it difficult to keep each user group separate. To isolate flows, enterprises must create thousands of separate tunnels or use highly complex virtualization techniques.

8

Lastly, tunnels create bottlenecks.

Tunnel architectures require a data center hub with branch spokes to backhaul all traffic to a central location. That means, yup, you guessed it, pinch points that increase latency and waste valuable bandwidth.

When it comes to tunnel technologies, the greatest hazard you face may be the toll imposed by the architecture itself. As the number of tunnels grows, traffic troubles are certain to follow.

There's a smarter way to route without troublesome tunnels. Learn more about Juniper's tunnel-free Session Smart Router.

Learn more

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000 | Fax: +1.408.745.2100
www.juniper.net

3050191-001-EN