
Topic / Issue: IPSEC VPN Packet loss- Bintec X series

Written By: Scott Young

If you are finding that certain packet types are not reaching the end point of your VPN tunnel, then Bintec suggest that you enable PMTU discovery.

To enable this you will need firmware version 6.3.4 or greater.
This firmware must be downloaded from Bintec's web site, under the IPSEC registration section.
(you must use an IPSEC enabled firmware, not a standard firmware)

MTU notes fro Bintec

Important hints for using PMTU Discovery in connection with IPsec and SIF

PMTU discovery has the aim to prevent/prohibit fragmentation over any LAN / WAN or Tunnel interface.

It does not matter wether the IP-packets are transmitted over leased lines, dialup-lines, IPsec tunnels or wether the internet is used or not.

The realization is rather simple:

- Every TCP/IP hosts system has the possibility to activate PMTU discovery
- When PMTU discovery is activated, this hosts sends every IP packet with the 'Dont fragment'-Flag set
- A router which has to route such a packet is not allowed to split this packet into fragments.
He must inform the sender of the packet, that it could not deliver the packet.
- This information is given to the sender of the packet via a ICMP packet (Type 3, Code 4), also called "destination unreachable, fragmentation needed" (see RFC 792)
- Within this ICMP packet the MTU which can be used is also delivered, so that the sender can lower the used MTU accordingly

Using a BinTec as IPsec Gateway makes this implementation a little bit more complex.

- if a host within the LAN sends a packet with e.g. size 1500 the BinTec would notice this at once
and will inform him about the lower MTU (because of the IPsec overhead) via a ICMP.
 - if the BinTec itself sends a packet via Internet and any router which has to route this IPsec packet (ESP packet)
would have to fragment it, this router will send a ICMP packet back to the BinTec
 - Because the ESP packet contains encrypted data the BinTec will only know which tunnel the original packet had belonged to,
but in this moment he does not know what the original sender was. So the BinTec remembers the max. MTU for this tunnel.
 - If another host within LAN wants to send a packet over this tunnel, he can inform this host at once.
-

IMPORTANT:

For ensuring PMTU discovery to work, one has to assure, that these ICMP packets are not filtered/blocked

- 1.) between the BinTec IPSec Gateway and the Internet (e.g. if the BinTec is located within a DMZ behind a firewall)
- 2.) between the BinTec IPSec Gateway and the hosts within the LAN.
- 3.) BinTec itself must not block the ICMP packets when arriving from Internet

Point 1.)

=====

must be configured on the firewall if any exists.

Point 2.)

=====

To ensure that the BinTec can transmit ICMP packets to hosts in the LAN, one has to configure the IPSec traffic list accordingly. This means, ICMPs send from the router must be allowed to be transmitted unencrypted.

If the PostIPSec-Defaulttrule is set to "pass" -> it should function anyway
If the PostIPSec-Defaulttrule is set to "drop it" -> there must be configured Pre-IPSec-Rules, which define that the router can route ICMP packets unencrypted.
There also must be a Pre-IPSec-Rule (which passes your local net unencrypted) if you have defined a traffic list with Remote Address "0.0.0.0".

The SIF (Stateful Inspection Firewall) never blocks ICMP packets originating from the router itself,
because all locally initiated sessions are allowed by SIF anyway.

Point 3.)

=====

For this point the implementation was adapted in the past. This means,

- a.) there is no NAT entry necessary to allow ICMP packets (type 3 code 4) arriving from the internet
- b.) there is no special entry necessary for IPSec -> the inbound IPSec filter catches this ICMP packet and computes the resulting MTU for this tunnel
- c.) there is no SIF entry necessary because this ICMP packet never reaches the SIF subsystem

Summary:
(If required)