

CLAIMS

1. A method for managing Internet Protocol Security (IPsec) for virtual private network (VPN) concentrators, the method comprising:
 - identifying, by at least one processor of an edge gateway backend system, a first IPsec tunnel between a VPN client and a VPN concentrator of the edge gateway backend system;
 - identifying, by the at least one processor, a second IPsec tunnel between the VPN client and the VPN concentrator;
 - identifying, by the at least one processor, a third IPsec tunnel between the VPN client and the VPN concentrator;
 - determining, by the at least one processor, that the first IPsec tunnel is a highest priority tunnel between the VPN client and the VPN concentrator;
 - determining, by the at least one processor, that the highest priority tunnel between the VPN client and the VPN concentrator is active; and
 - deactivating, by the at least one processor, fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel from the VPN concentrator based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator is active.
2. The method of claim 1, wherein the second IPsec tunnel and the third IPsec tunnel are inactive at the VPN concentrator based on the highest priority tunnel between the VPN client and the VPN concentrator being active.
3. The method of claim 1 or 2, further comprising:
 - determining that the highest priority tunnel between the VPN client and the VPN concentrator is inactive; and
 - adding, based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator is inactive, the fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel to the VPN concentrator.
4. The method of claim 3, further comprising:
 - determining that the highest priority tunnel between the VPN client and the VPN concentrator has become active after being inactive; and

deactivating, based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator has become active after being inactive, the fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel from the VPN concentrator.

5. The method of any preceding claim, further comprising:
identifying a fourth IPsec tunnel between a second VPN client and the VPN concentrator;
identifying a fifth IPsec tunnel between the second VPN client and the VPN concentrator;
identifying a sixth IPsec tunnel between the second VPN client and the VPN

concentrator;

determining that the fourth IPsec tunnel is a highest priority tunnel between the second VPN client and the VPN concentrator;

determining that the highest priority tunnel between the second VPN client and the VPN concentrator is active; and

deactivating fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel from the VPN concentrator based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator is active.

6. The method of claim 5, further comprising:

determining that the highest priority tunnel between the second VPN client and the VPN concentrator is inactive; and

adding, based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator is inactive, the fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel to the VPN concentrator,

the method preferably further comprising:

determining that the highest priority tunnel between the second VPN client and the VPN concentrator has become active after being inactive; and

deactivating, based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator has become active after being inactive, the fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel from the VPN concentrator.

7. The method of any preceding claim, further comprising determining a maximum number of active IPsec tunnels to be maintained by the VPN concentrator,

the method preferably further comprising determining a maximum number of VPN clients that may connect to the VPN concentrator based on the maximum number of active IPsec tunnels to be maintained by the VPN concentrator.

8. A system for managing Internet Protocol Security (IPsec) for virtual private network (VPN) concentrators, the system comprising memory coupled to at least one processor of an edge gateway backend system, the at least one processor configured to:

identify a first IPsec tunnel between a VPN client and a VPN concentrator of the edge gateway backend system;

identify a second IPsec tunnel between the VPN client and the VPN concentrator;

identify a third IPsec tunnel between the VPN client and the VPN concentrator;

determine that the first IPsec tunnel is a highest priority tunnel between the VPN client and the VPN concentrator;

determine that the highest priority tunnel between the VPN client and the VPN concentrator is active; and

deactivate fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel from the VPN concentrator based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator is active.

9. The system of claim 8, wherein the second IPsec tunnel and the third IPsec tunnel are inactive at the VPN concentrator based on the highest priority tunnel between the VPN client and the VPN concentrator being active.

10. The system of claim 8 or 9, wherein the at least one processor is further configured to:
determine that the highest priority tunnel between the VPN client and the VPN concentrator is inactive; and

add, based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator is inactive, the fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel to the VPN concentrator.

11. The system of claim 10, wherein the at least one processor is further configured to:
 - determine that the highest priority tunnel between the VPN client and the VPN concentrator has become active after being inactive; and
 - deactivate, based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator has become active after being inactive, the fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel from the VPN concentrator.
12. The system of any one of claims 8 to 11, wherein the at least one processor is further configured to:
 - identify a fourth IPsec tunnel between a second VPN client and the VPN concentrator;
 - identify a fifth IPsec tunnel between the second VPN client and the VPN concentrator;
 - identify a sixth IPsec tunnel between the second VPN client and the VPN concentrator;
 - determine that the fourth IPsec tunnel is a highest priority tunnel between the second VPN client and the VPN concentrator;
 - determine that the highest priority tunnel between the second VPN client and the VPN concentrator is active; and
 - deactivate fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel from the VPN concentrator based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator is active.
13. The system of claim 12, wherein the at least one processor is further configured to:
 - determine that the highest priority tunnel between the second VPN client and the VPN concentrator is inactive; and
 - add, based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator is inactive, the fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel to the VPN concentrator,
 - preferably wherein the at least one processor is further configured to:
 - determine that the highest priority tunnel between the second VPN client and the VPN concentrator has become active after being inactive; and

deactivate, based on the determination that the highest priority tunnel between the second VPN client and the VPN concentrator has become active after being inactive, the fully qualified domain names of the fifth IPsec tunnel and the sixth IPsec tunnel from the VPN concentrator.

14. The system of any one of claims 8 to 13, wherein the at least one processor is further configured to determine a maximum number of active IPsec tunnels to be maintained by the VPN concentrator,

preferably wherein the at least one processor is further configured to determine a maximum number of VPN clients that may connect to the VPN concentrator based on the maximum number of active IPsec tunnels to be maintained by the VPN concentrator.

15. A computer program comprising instructions to cause at least one processor of an edge gateway backend system for managing Internet Protocol Security (IPsec) for virtual private network (VPN) concentrators, upon execution of the instructions by the at least one processor, to:

identify a first IPsec tunnel between a VPN client and a VPN concentrator of the edge gateway backend system;

identify a second IPsec tunnel between the VPN client and the VPN concentrator;

identify a third IPsec tunnel between the VPN client and the VPN concentrator;

determine that the first IPsec tunnel is a highest priority tunnel between the VPN client and the VPN concentrator;

determine that the highest priority tunnel between the VPN client and the VPN concentrator is active; and

deactivate fully qualified domain names of the second IPsec tunnel and the third IPsec tunnel from the VPN concentrator based on the determination that the highest priority tunnel between the VPN client and the VPN concentrator is active,

preferably wherein the second IPsec tunnel and the third IPsec tunnel are inactive at the VPN concentrator based on the highest priority tunnel between the VPN client and the VPN concentrator being active.