CCIE Security Version 5 Advanced Technologies Class

ACL Troubleshooting

Why doesn't my RACL work?

RACL Troubleshooting

▷ A router ACL is known as a RACL

- IP ACL applied inbound/outbound on a router interface

▷ If your RACL policy is not enforced

- Ensure the ACL is properly configured (more specific entries are at the top of the ACL)
- Ensure the ACL is applied and in the proper direction and proper interface
- Inbound ACL matches on all traffic, outbound ACL only on transit traffic by default

RACL Troubleshooting

▷If your RACL policy is still not enforced

- Ensure the packet is an IP packet (not as an MPLS packet for example)

- Validate object-group configuration

- Ensure the ACL name/number and/or object-group name exists

- Explicitly configure a deny statement at the end of the ACL, with logging enabled, see if it matches

Knowledge is Power!