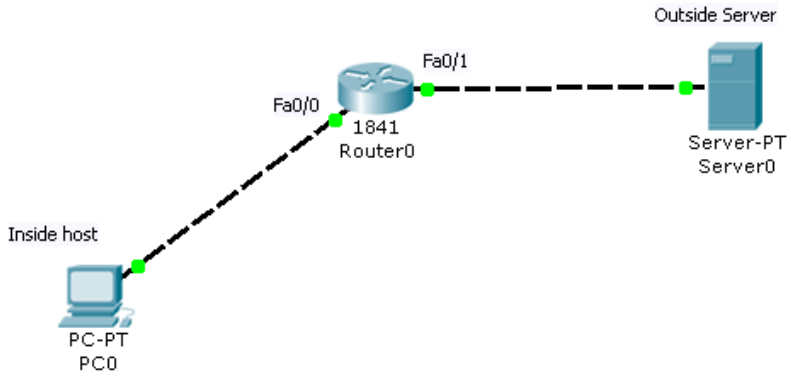
Context Based Access Control (CBAC)

So, In essence, the router checks any outgoing traffic and decides if it will allow answers back in to the protected “inside” network.

What you do is decide “What protocol from what inside interface will I allow answers back to? (the Context)”

Ping (ICMP) example between inside host and outside server.



First we need to block traffic we do not want to be initialized from the outside. Usual case is all traffic.

Create block for incoming traffic
ip access-list extended LOCKOUT
deny ip any any

Apply that rule to the outer interface for traffic coming IN.

Apply to outer interface, inbound
interface fa0/1
ip access-group LOCKOUT in

Now we need to add inspection rules to the protocols we’d like to be initialized from the inside.

Create inspection rule to allow ICMP requests from the inside
ip inspect name ICMP icmp

We want the router to register all packets with matching protocol (ICMP) on the inside interface (coming IN to the router) and allow replies to it.

Apply to inner interface, inbound
interface fa0/0
ip inspect ICMP in
(*another option would be to look at the ones going OUT from Fa0/1)*

Try debugging while pinging between the inside host and the outside server

Debug inspected ICMP traffic
debug ip inspect protocol icmp