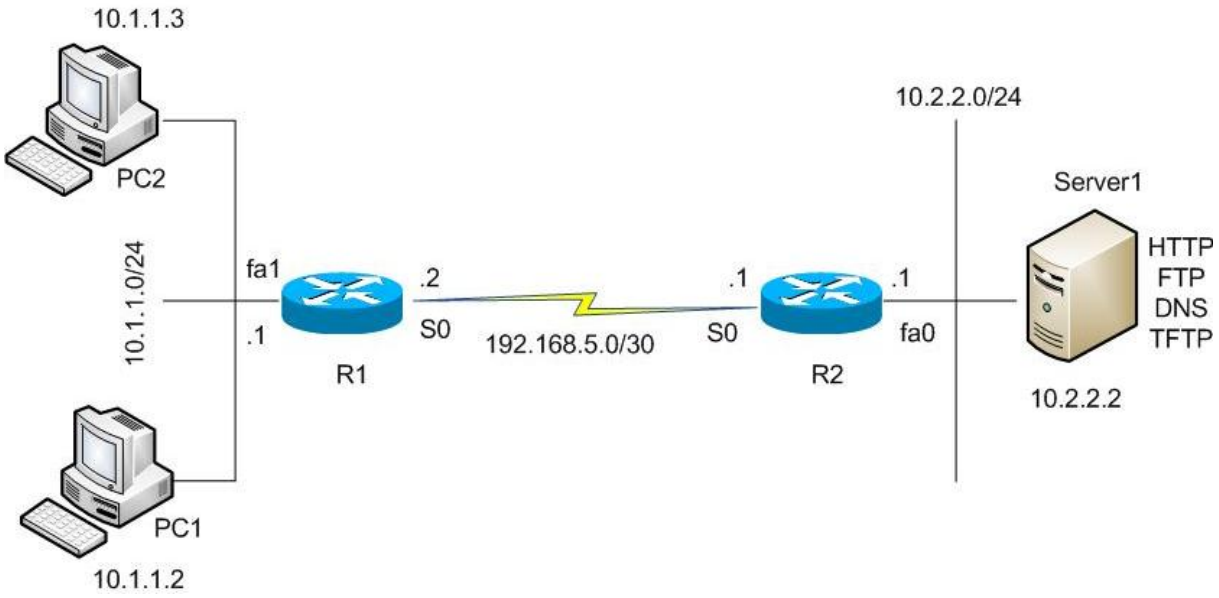
Komplettaufgabe: Access Control Lists (ACLs)

Die folgenden praktischen Aufgaben basieren auf dem nachfolgend gezeigten Lab:



Theorie:

1. Welche Nummernbereiche definieren Standard-ACLs?
2. Welche Filtermöglichkeiten existieren mit Standard-ACLs?
3. Wo sollten Standard-ACLs am besten platziert werden und warum?
4. Wieviele ACLs können pro Interface zugeordnet werden?
5. Welche Grundregel in der Reihenfolge sollten Sie beim Erstellen von ACLs beachten?
6. Welche letzte Regel ist in jeder ACL enthalten?
7. Welche Schlüsselwörter können Sie in ACLs platzieren?
8. Welche Nummernbereiche definieren Extended-ACLs?
9. Nennen Sie mindestens 4 Filtermöglichkeiten für Extended-ACLs.
10. Wo sollten Extended ACLs am besten platziert werden und warum?
11. Wann würden Sie Inbound-Filter und wann Outbound-Filter nutzen?
12. Wie werden Named-ACLs festgelegt? Haben Named-ACLs Nummernbereiche?
13. Mit welchem Befehl (und in welchem Subconfig-Mode) werden Zugriffe auf den Router selbst kontrolliert?

Praxis:

1. Erstellen Sie eine Standard-ACL, mit der Zugriffe vom Netzwerk 10.1.1.0/24 auf das Netzwerk 10.2.2.0/24 nicht gestattet werden, alles andere aber schon. Wo müssen Sie diese ACL aktivieren?
2. Testen Sie den Zugriff auf Server1 von einem der PCs und von R1 per Ping. Welche Kommunikation kommt zustande?
3. Analysieren Sie die ACL-Treffer. Wie viele Treffer sind vorhanden und was sagen Sie aus?
4. Entfernen Sie die Zuordnung der ACL zum Interface und testen Sie den Zugriff erneut. Diesmal müssen die Pings auch von den PCs beantwortet werden.

5. Erstellen Sie eine Extended ACL auf dem geeigneten Router, die folgende Bedingungen erfüllt:
    a. Ping von PC2 auf alle Ziele: erlaubt
    b. Ping von PC1 auf Server1: erlaubt
    c. Ping von allen anderen Systemen aus dem Netz 10.1.1.0/24: verboten
    d. Telnet von PC1 auf R2: erlaubt
    e. http von allen Systemen auf Server1: erlaubt
    f. http von PC2 auf R2: erlaubt
    g. Kommunikation über http, Ping und Telnet von allen anderen Systemen: verboten
    h. Kommunikation über FTP von allen Systemen auf alle Systeme: erlaubt
6. Weisen Sie diese ACL dem geeigneten Interface zu und testen Sie die ACL ausgiebig.
7. Entfernen Sie die ACL von dem Interface und testen Sie den Zugriff erneut. Jetzt muss jede Kommunikation zustande kommen.
8. Erstellen Sie eine Named ACL namens GULUGULU, die folgende Bedingungen erfüllt:
    a. FTP auf Server1 von PC1: erlaubt
    b. Telnet auf R2 vom PC2: erlaubt
    c. Telnet von allen anderen Systemen aus dem Netz 10.1.1.0/24: verboten
    d. Ping auf alle Systeme vom Netz 10.1.1.0/24: erlaubt
9. An der 2. Stelle der ACL soll eine weitere Regel eingefügt werden, wonach TFTP von PC1 auf R2 erlaubt sein soll. Ändern Sie die ACL entsprechend ab.
10. Sie stellen fest, dass nicht Telnet, sondern SSH vom PC2 erlaubt werden soll – ändern Sie die ACL entsprechend, in dem Sie die vorhandenen Zeilen ersetzen, ohne die Reihenfolge der Regeln zu ändern.
11. Weisen Sie die ACL dem richtigen Interface zu und testen Sie das Ergebnis.
12. Entfernen Sie die ACL wieder von diesem Interface.
13. Sorgen Sie über einen geeigneten Weg dafür, dass ausschließlich PC1 als Admin-PC per Telnet oder SSH auf R2 zugreifen kann. Dabei darf es keine Rolle spielen, über welches Interface des Routers PC1 zugreift.