

Praktikum 5 zur Vorlesung IT-Sicherheit

Thema Firewalling

1 Installation von Packet-Tracer

Dieser Versuch erfolgt auf Basis von Packet-Tracer. Packet-Tracer ist das Cisco Simulationstool für Netzwerke. Besorgen Sie sich Packet-Tracer, z.B. indem Sie sich unter www.netacad.com/courses/intro-packet-tracer/ für den Selbstlern-Kurs „**Introduction to Packet Tracer**“ (kostenlos) einschreiben. Dann können Sie Packet-Tracer herunterladen und installieren.

Machen Sie sich mit der Funktionsweise von Packet-Tracer vertraut.

Die Versuchstopologie finden Sie im Lernraum der Vorlesung IT-Sicherheit in der Datei „*ITS P5 PT-Netztopologie.pkt*“. Öffnen Sie die Datei mit Packet-Tracer.

Hier die wichtigsten Funktionen, die für die Aufgabe benötigt werden:

Router Kommandozeile

Klicken Sie auf den ausgewählten Router.

Gehen Sie auf CLI (Command Line Interface).

Klicken Sie in das Kommandofenster. Jetzt können Sie den Router konfigurieren.

Mit **enable** (kurz **en**) gelangen Sie in den Privileged-Mode, von dort mit **config terminal** (kurz **conf t**) in den globalen Konfigurationsmodus. Mit **exit** gelangen Sie jeweils wieder zurück.

PC / Server Bedienung

Klicken Sie auf den ausgewählten PC oder Server.

Gehen Sie auf Desktop.

- Unter IP-Configuration können Sie die IP-Konfiguration einsehen.
- Unter Command Prompt können Sie Kommandos wie z.B. ping und telnet durchführen.
- Unter Web Browser können Sie Webseiten abrufen, per http oder auch https.

Durch Schließen der Auswahl (X im Blauen Balken) gelangen Sie zurück zum Desktop.

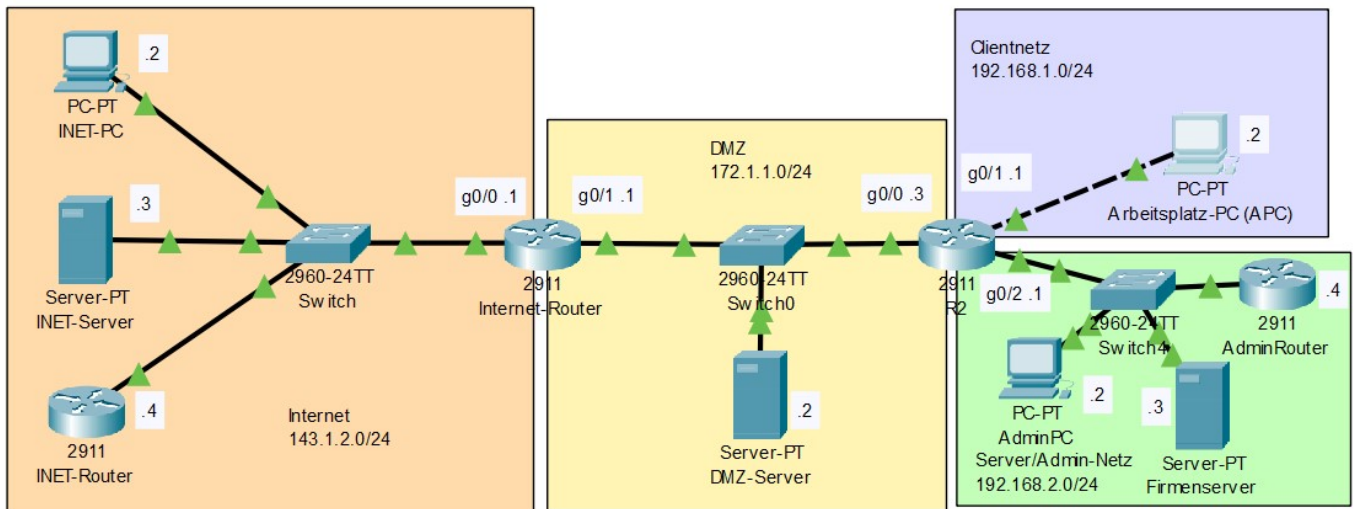
Im Folgenden wird davon ausgegangen, dass Sie Packet-Tracer nutzen können.

2 Zur Netztopologie für den Versuch

Im Rahmen der Übung soll ein Unternehmensnetz (s. nachstehende Abbildung) mit ACLs abgesichert werden. Das Unternehmen verfügt über

- ein Server/Adminnetz (192.168.2.0/24),
- ein Clientnetz (192.168.1.0/24),
- eine Demilitarisierte Zone (DMZ, 172.17.1.0/24), in der u.a. Web- und der DNS-Server betrieben werden.

Die DMZ ist über den Internet-Router des Unternehmens an das Internet (hier simuliert durch das Netz 143.1.2.0/24) angebunden. Zu den internen Netzen hin gibt es einen weiteren Router (R2).



Die Topologie ist aktuell so konfiguriert, dass vollständige Konnektivität gegeben ist. Die Konfigurationen der Router sind zur Information im Anhang angegeben. Diese werden jedoch zur Bearbeitung der Aufgabe nicht benötigt.

Die Komponenten in den Netzen haben folgende IP-Konfiguration:

Komponente	IP-Adresse	Standard-GW
INET-PC	143.1.2.2	143.1.2.1
INET-Server	143.1.2.3	143.1.2.1
INET-Router	143.1.2.4	
DMZ-Server	172.1.1.2	172.1.1.1 (!)
Arbeitsplatz-PC (kurz APC)	192.168.1.2	192.168.1.1
Admin-PC	192.168.2.2	192.168.2.1
Firmenserver	192.168.2.3	192.168.2.1
AdminRouter	192.168.2.4	

(Hinweis: AdminRouter und INET-Router dienen nur zum Austesten von telnet-Zugriffen, da Packet-Tracer kein telnet/ssh-Zugriff auf Server unterstützt.)

Der DMZ-Server dient als DNS-Server und hat Einträge für die 3 Server sowie INET- und Admin-Router.

3 Vorbereitung: Test der Konnektivität.

Für die Router wird als telnet-Passwort *cisco* und als enable-PW *class* verwendet.

Im Ausgangszustand sind keine ACLs auf den Routern. Testen Sie, dass vollständige Erreichbarkeit gegeben ist. Haken Sie Tests in den Tabellen unter OK? ab.

Hinweis: Bis es zu erfolgreichen Antworten kommt, kann es in der Packet-Tracer Simulation etliche Sekunden dauern!

3.1 Test der Erreichbarkeit der Rechner per ping

Testen Sie, dass die Rechner sich per ping erreichen können
(=> Desktop => Command Prompt)

Von	Ziel	Kommando	Ok?
INET-PC	APC	ping 192.168.1.2	
INET-PC	Firmenserver	ping firmenserver	
INET-PC	DMZ-Server	ping dmz-server	
APC	INET-PC	ping 143.1.2.2	
APC	INET-Server	ping inet-server	
APC	DMZ-Server	ping dmz-server	

3.2 Test der Erreichbarkeit der Web-Server

Auf jedem der 3 Server läuft ein WebServer. Testen Sie, dass alle Webserver vom INET-PC und APC zugreifbar sind (=> Desktop => Web-Browser):

Von	Ziel	URL	Ok?
INET-PC	Firmenserver	http://firmenserver	
INET-PC	DMZ-Server	http://dmz-server	
APC	Firmenserver	http://firmenserver	
APC	DMZ-Server	http://dmz-server	
APC	INET-Server	http://inet-server	

3.3 Test der Erreichbarkeit per telnet

Für die Aufgabe nutzen wir der Einfachheit halber telnet anstelle von SecureShell. In der Realität sollten sie niemals telnet verwenden!

Testen Sie, dass der AdminRouter und der INET-Router per telnet vom APC und INET-PC erreichbar sind. Loggen Sie sich mit dem Passwort cisco ein.

Von	Ziel	Kommando	Ok?
INET-PC	AdminRouter	telnet adminrouter	
APC	AdminRouter	telnet adminrouter	
APC	INET-Router	telnet inet-router	
DMZ-Server	AdminRouter	telnet adminrouter	

3.3 Test der Erreichbarkeit per DNS

Wenn die Aufrufe (ping, telnet, URL) per Namensangabe geklappt haben, ist klar, dass der DNS-Server auf dem DMZ-Server vom INET-PC und APC erreichbar ist.

4 Umsetzung einer Network Security Policy

Die Network Security Policy des Unternehmens enthält folgende Vorgaben:

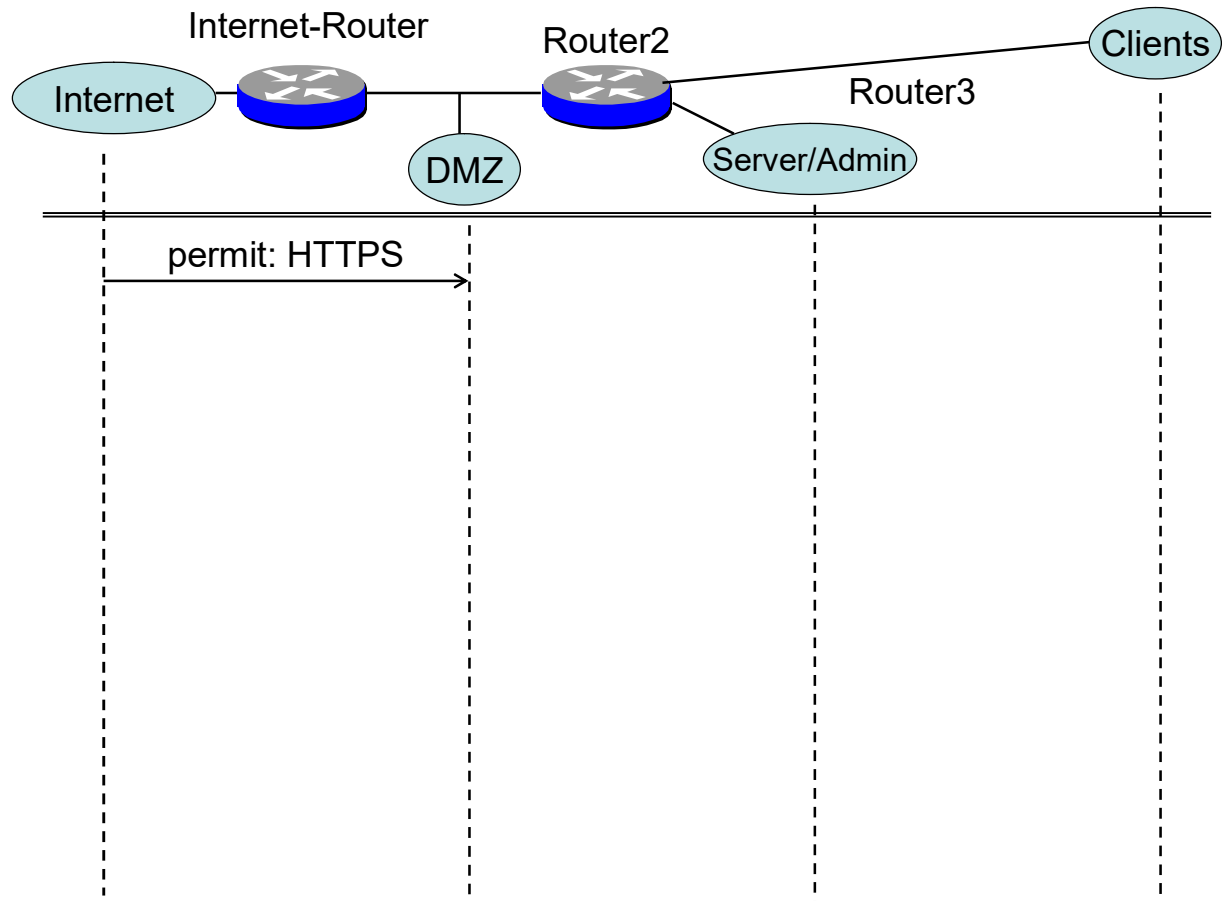
1. Bis auf https soll die Firma vom Internet aus nicht sichtbar sein. Außer dem https-Zugriff auf die DMZ sind keine Verbindungsaufbauten von außen nach innen erlaubt. Sämtlicher anderer Netzverkehr (auch Pings und DNS-Abfragen) ist zu blockieren.
2. Die internen Netze (Clientnetz und Server/Adminnetz) sind zweistufig gegenüber dem Internet abzusichern. Die Absicherung ist so vorzunehmen, dass im Falle der Kompromittierung des Internet-Routers die internen Netze weiterhin mit gleicher Filterfunktionalität geschützt sind. Auch Pings sollen weiterhin nicht nach innen gelangen.
3. Aufgrund des hohen Schutzbedarfs des Server/Adminnetzes ist es erforderlich, dass sämtliche Zugriffe vom Server/Adminnetz auf das Internet über Proxies in der DMZ laufen. Aus Sicherheitsgründen sind daher jegliche *direkte* Zugriffe vom Server/Adminnetz auf das Internet zu sperren!
4. PCs im Clientnetz dürfen nicht zur Serveradministration eingesetzt werden. Entsprechend sind Zugriffe aus dem Clientnetz per telnet (Port 23) und SSH (Port 22) auf die DMZ und das Server/Adminnetz zu sperren. Sämtlicher andere IP Verkehr ist zu erlauben.

In Aufgaben 4.1 sollen Sie die Kommunikationsbeziehungen (erlaubte und gesperrte) gemäß der Policy in einem Diagramm dokumentieren.

Anschließend sollen Sie in Aufgabe 4.2 die Policy durch Konfiguration von ACLs auf dem Internet-Router und dem Router 2 implementieren.

4.1 Aufgabe: Kommunikationsbeziehungen (erlaubte und gesperrte) dokumentieren

Zeichnen sie die gemäß Network Security Policy *erlaubten* und *zu sperrenden* Kommunikationsverbindungen als beschriftete Pfeile in die nachstehende Abbildung ein. Die Pfeilspitze gibt dabei die Richtung des Verbindungsaufbaus an. Berücksichtigen Sie, dass in der Policy nicht explizit erwähnten Kommunikationsbeziehungen erlaubt sein sollen. Insbesondere ist es zulässig, aus dem Clientnetz Verbindungen ins Internet aufzubauen.



4.2 Aufgabe: Umsetzung der Policy auf dem Internet-Router und Router R2

Implementieren Sie die Network Security Policy durch Konfiguration von ACLs und CBAC-Regeln auf dem Internet-Router und Router R2 unter Beachtung folgender Randbedingungen:

- Nehmen Sie Konfigurationsänderungen nur am Internet-Router und Router R2 vor und sonst an keinem anderen Gerät.
- In der Topologie erfolgt das Routing mit RIPv2. Damit das RIPv2-Routing funktioniert die RIP-Kommunikation global immer in der ersten Regel jeder ACL freigeben:
`permit udp any any eq 520`
- Verwenden Sie Extended ACLs mit Namen.
- Realisieren Sie das Zulassen von TCP/UDP-Antworten auf intern initiierte TCP/UDP-Anfragen durch CBAC-Regeln (inspect ...).

- Das Internet wird in der Topologi zwar durch das Netz 143.1.2.0/24 simuliert, es soll jedoch in den ACLs **ausschließlich** mit *any* adressiert werden.
- (Wenn eindeutig ist, aus welchem Netz Pakete kommen, kann auch die Quelle als *any* angegeben werden.)
- Dringende Empfehlung: Editieren Sie die Kommandos zur Konfiguration der Regeln in einer Textdatei. Kopieren Sie die Kommandos blockweise ins Router CLI (Rechte Moustaste => Paste). Denken Sie daran, dass beim Wiederaufruf einer ACL Regeln am Ende der ACL ergänzt werden. Daher empfiehlt es sich, jeweils zunächst die ACL zu Löschen (no ip access-list) und dann komplett neu anzulegen.

Weitere Hinweise zu den ACLs, die Ihnen die Arbeit erleichtern, finden Sie im Anhang.

Aber überlegen Sie gerne zunächst selbst, welche Regeln Sie für welche Interfaces vorsehen.

Platz zur Dokumentation der Lösung finden Sie nach Abschnitt 5.

5 Prüfung der Umsetzung der Network Security Policy

Zu den Vorgaben der Policy stehen in den folgenden Tabellen jeweils Tests inkl. Soll-Verhalten bzw. Soll-Funktion, um die Schutz-Funktion zu prüfen.

Prüfen Sie, ob der Soll-Schutz gemäß der Policy gegeben ist. Falls nicht, suchen Sie den Fehler und testen Sie erneut. Am Ende sollte die jeweilige Soll-Funktion gegeben sein.

1. Bis auf https soll die Firma vom Internet aus nicht sichtbar sein. Außer dem https-Zugriff auf die DMZ sind keine Verbindungsaufbauten von außen nach innen erlaubt. Sämtlicher anderer Netzverkehr (inkl. Pings und DNS-Abfragen) ist zu blockieren.

Wir prüfen mit IP-Adressen, da der DNS-Server aus dem Internet nicht erreichbar ist.

Zugriffe aus dem Internet (INET-PC)	Soll-Funktion	OK?
Browser: http://172.1.1.2 (DMZ-Server)	Geblockt	
Browser: https://172.1.1.2 (DMZ-Server)	Erlaubt	
Ping 172.1.1.2 (DMZ-Server)	Geblockt	
telnet 192.168.2.4 (AdminPC)	Geblockt	
Browser: https://192.168.2.3 (Firmenserver)	Geblockt	

2. Die internen Netze (Clientnetz und Server/Adminnetz) sind zweistufig gegenüber dem Internet abzusichern. Die Absicherung ist so vorzunehmen, dass im Falle der Kompromittierung des Internet-Routers die internen Netze weiterhin mit gleicher Filterfunktionalität geschützt sind. Insbesondere sollen Pings aus dem Internet weiterhin nicht nach innen gelangen.

Also sollen auch aus der DMZ heraus die internen Netze nicht erreichbar sein.

Zugriffe aus der DMZ (DMZ-Server)	Soll-Funktion	OK?
ping 192.168.1.2 (Arbeitsplatz PC)	Geblockt	
ping firmenserver	Geblockt	
ping inet-server	Erlaubt	
Browser: http://firmenserver	Geblockt	
Browser: http://inet-server	Erlaubt	
telnet adminrouter	Geblockt	
telnet inet-router	Erlaubt	

3. Aufgrund des hohen Schutzbedarfs des Server/Adminnetzes ist es erforderlich, dass sämtliche Zugriffe vom Server/Adminnetz auf das Internet über Proxies in der DMZ laufen. Aus Sicherheitsgründen sind daher jegliche *direkte* Zugriffe vom Server/Adminnetz auf das Internet zu sperren!

Zugriffe aus dem Server/Adminnetz (Admin-PC)	Soll-Funktion	OK?
nslookup inet-server => Ausgabe: 143.1.2.3	Funktioniert	
ping inet-server	Geblockt	
telnet inet-router	Geblockt	
Browser: http://inet-server	Geblockt	
ping 192.168.1.2 (Arbeitsplatz PC)	Erlaubt	
Browser: http://dmz-server	Erlaubt	

4. PCs im Clientnetz dürfen nicht zur Serveradministration eingesetzt werden. Entsprechend sind Zugriffe aus dem Clientnetz per telnet (Port 23) und SSH (Port 22) auf die DMZ und das Server/Adminnetz zu sperren. Sämtlicher andere IP Verkehr ist zu erlauben.

Zugriffe aus dem Clientnetz (Arbeitsplatz PC)	Soll-Funktion	OK?
nslookup inet-server => Ausgabe: 143.1.2.3	Funktioniert	
ping inet-server	Erlaubt	
telnet inet-router	Erlaubt	
Browser: http://inet-server	Erlaubt	
Browser: http://firmenserver	Erlaubt	
ping adminrouter	Erlaubt	
telnet adminrouter	Geblockt	

6 Platz zur Dokumentation der Lösung

Router: Internet-Router	Interface: Internet (g0/0)	Filterrichtung: Eingehend: Internet->DMZ
-------------------------	----------------------------	---

```
! Access-List INET_IN fuer Kommunikation vom Internet in die DMZ
! Auf gi0/0 (Internet) des Internet-Routers eingehend filtern
ip access-list extended INET_IN
    ! RIP global freigeben
    permit udp any any eq 520
    ! Hier weitere Regel(n) ergaenzen
```


exit

```
! ACL INET_IN dem Interface g0/0 eingehend zuweisen
interface g0/0
    ip access-group INET_IN in
exit
```

```
! Hier Regeln INET_ALLOW zur dynamischen Freigabe
! des Ruckverkehrs ergaenzen
```


```
! Inspect Regeln INET_ALLOW g0/0 zuweisen
interface g0/0
    ip inspect INET_ALLOW out
exit
```


Router: R2	Interface: g0/0	Filterrichtung: eingehend (DMZ -> interne Netze)
------------	-----------------	---

! Access-List DMZ_IN fuer Kommunikation von der DMZ nach intern

! Access-List DMZ_IN dem Interface zuweisen

! Rückverkehr mit Regel DMZ_ALLOW dynamisch freigeben

! Regel DMZ_IN dem Interface zuweisen

Router: R2	Interface: g0/2	Filterrichtung: eingehend (Server/Adminnetz -> andere Netze)
------------	-----------------	--

**! Access-List ADMIN_NO_INET zur Sperrung von Zugriffen
! auf das Internet (= any)**

! Access-List ADMIN_NO_INET dem Interface zuweisen

Router: R2	Interface: g0/1	Filterrichtung: eingehend (Clientnetz -> andere Netze)
------------	-----------------	--

**! Access-List NO_SSH_TELNET zur Sperrung von
! SSH- und telnet-Zugriffen auf das Admin/Servernetz**

! Access-List NO_SSH_TELNET dem Interface zuweisen

7 Anhang: Hinweise zur ACL Regelkonfiguration:

1. Bis auf HTTPS soll die Firma vom Internet aus nicht sichtbar sein. Außer dem HTTPS-Zugriff auf die DMZ sind keine Verbindungsaufbauten von außen nach innen erlaubt. Sämtlicher anderer Netzverkehr (auch Pings und DNS-Abfragen) ist zu blockieren.
=> Internet-Router: Für das Internet-Interface g0/0 eingehend eine ACL namens INET_IN konfigurieren, die nur HTTPS für das DMZ-Netz freigibt (und RIP global) und sonst alles sperrt. Die ACL dem Interface eingehend zuweisen.
=> Internet-Router: Rückverkehr aus dem Internet per inspect-Regeln namens INET_ALLOW freigeben und diese g0/0 eingehend zuweisen.
2. Die internen Netze (Clientnetz und Server/Adminnetz) sind zweistufig gegenüber dem Internet abzusichern. Die Absicherung ist so vorzunehmen, dass im Falle der Kompromittierung des Internet-Routers die internen Netze weiterhin mit gleicher Filterfunktionalität geschützt sind. Auch Pings sollen weiterhin nicht nach innen gelangen.
=> R2: Für das DMZ-Interface g0/0 eingehend eine ACL namens DMZ_IN konfigurieren, die alles (außer RIP) sperrt. Die ACL dem Interface eingehend zuweisen.
=> R2: Rückverkehr aus der DMZ in die internen Netze per inspect-Regeln namens DMZ_IN_ALLOW freigeben und diese g0/0 eingehend zuweisen. Auch DNS Rückverkehr soll möglich sein!
3. Aufgrund des hohen Schutzbedarfs des Server/Adminnetzes ist es erforderlich, dass sämtliche Zugriffe vom Server/Adminnetz auf das Internet über Proxies in der DMZ laufen. Aus Sicherheitsgründen sind daher jegliche *direkte* Zugriffe vom Server/Adminnetz auf das Internet zu sperren!
=> R2: Für das Interface g0/2 zum Server/Adminnetz eingehend eine ACL mit dem Namen ADMIN_NO_INET konfigurieren, die Zugriffe auf das Internet (= any) sperrt. Zugriffe auf die anderen beiden Netze sollen weiterhin möglich sein! Die ACL dem Interface g0/2 eingehend zuweisen.
4. PCs im Clientnetz dürfen nicht zur Serveradministration eingesetzt werden. Entsprechend sind Zugriffe aus dem Clientnetz per telnet (Port 23) und SSH (Port 22) auf die DMZ und das Server/Adminnetz zu sperren. Sämtlicher andere IP Verkehr ist zu erlauben.
=> R2: Für das Interface g0/1 zum Clientnetz eingehend eine ACL mit dem Namen NO_SSH_TELNET konfigurieren, die telnet und SSH Zugriffe auf das Server-/Adminnetz sperrt (und alles andere erlaubt). Die ACL dem Interface g0/1 eingehend zuweisen.

8 Anhang: Routerkonfigurationen (rein informativ)

Internet-Router hostname Internet-Router no ip domian-lookup interface GigabitEthernet0/0 description Internet-Interface ip address 143.1.2.1 255.255.255.0 no shutdwon interface GigabitEthernet0/1 description DMZ-Interface ip address 172.1.1.1 255.255.255.0 no shutdown line vty 0 15 password cisco login router rip version 2 network 143.1.0.0 network 172.1.0.0	Router R2 hostname R2 no ip domian-lookup interface GigabitEthernet0/0 description DMZ-Interface ip address 172.1.1.3 255.255.255.0 no shutdown interface GigabitEthernet0/1 description Clientnetz-Interface ip address 192.168.1.1 255.255.255.0 no shutdown interface GigabitEthernet0/2 description Server/Adminnetz-Interface ip address 192.168.2.1 255.255.255.0 no shutdown line vty 0 15 password cisco login router rip version 2 network 192.168.1.0 network 192.168.2.0 network 172.1.1.0
Adminrouter hostname AdminRouter banner motd #!!! Hier haben nur Admin der Fa. Zugriff !!!# no ip domain lookup int g0/0 ip address 192.168.2.4 255.255.255.0 no shutdown line vty 0 15 password cisco login enable secret class router rip version 2 network 192.168.2.0	INET-Router hostname INET-Router no ip domain lookup int g0/0 ip address 143.1.2.4 255.255.255.0 no shutdown line vty 0 15 password cisco login enable secret class router rip version 2 network 143.1.2.0