AAA - Authentication-Authorization-Accounting

Studiengang:	Medieninformatik WiSe15/16
Modul:	Informationssicherheit - Labor
Laborgruppe:	Gruppe Z (C)
Bericht von:	Arthur Jaks
	Tobias Winkler
	Emel Altmisoglu

Inhaltsangabe

Einleitung

Um in einem Netzwerk bestimmte Sicherheitsschritte zu gewährleisten, wurde das AAA System entwickelt.
Das sogenannte „Tripple A“ System, beschreibt den Vorgang für eine intelligente Steuerung des Zugriffs auf Computerressourcen, die Einhaltung bestimmter Richtlinien, die Überwachung der Nutzung sowie die Bereitstellung Abrechnungsrelevanter Services .

Das erste A steht für **Authentifizierung** und bietet die Möglichkeit der Identifizierung des Benutzers.
Dazu muss der Benutzer einen gültigen Benutzernamen eingeben und ein gültiges Passwort bevor der Zugriff gewährt wird.
Ein AAA-Server vergleicht die eingegebenen Daten mit denen in seiner Datenbank.
Stimmen diese über ein wird der Zugriff gewährt

Nach der Authentifizierung folgt üblicherweise die **Autorisierung**, d.H. dem Benutzer werden bestimmte Privilegien zugesprochen.
Das System überprüft somit, was der Benutzer darf und mit welchen Ressourcen.

Das letzte A beschreibt den **Abrechnung**sprozess, dabei werden die vom Benutzer verbrauchten Ressourcen gemessen, wie z.B. die Länge der Sitzungsdauer oder die Größe der Daten die ein Benutzer empfangen oder gesendet hat.
Diese Messungen dienen dazu, um Statistiken zu erstellen für zukünftige Kapazitätsplanungen, Trendanalysen oder Rechnungen zu erstellen.

Die Aufgabe des folgenden Versuches besteht darin, ein solches AAA-Framework in einem vorgegeben Netzwerk zu installieren.

Versuchsaufbau

Auf Abb. 2 ist ein fertig konfiguriertes Netzwerk zu sehen.

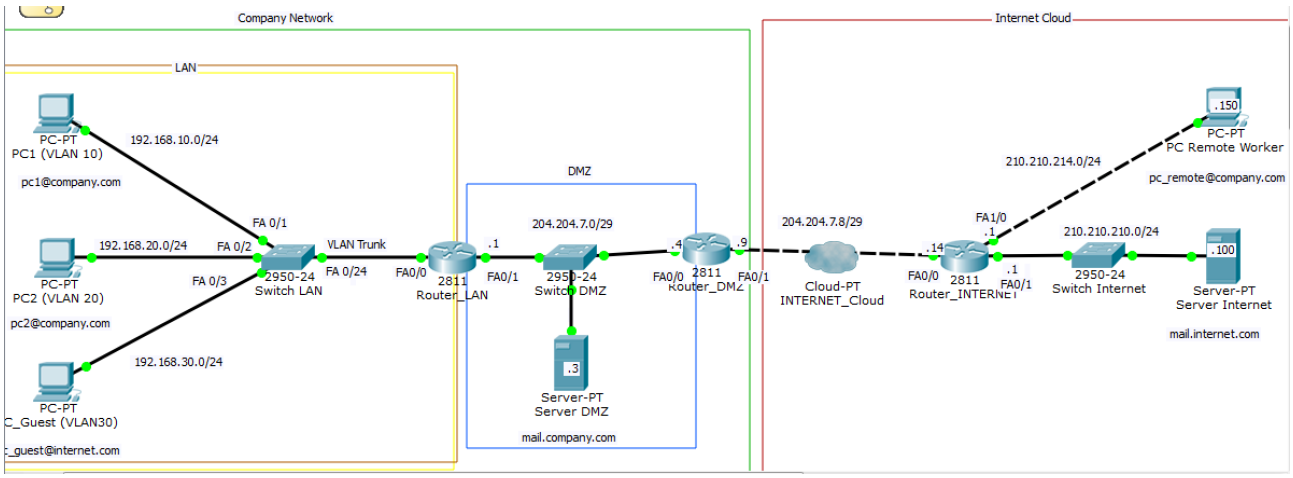

Abb. 2: Fertig konfiguriertes Netzwerk.

Das Netzwerk ist in 3 Bereiche aufgeteilt: LAN, DMZ und Internet Cloud.
Für den Versuch sind momentan aber nur Bereich LAN und DMZ relevant.
Das LAN-Netzwerk ist wie folgt von links nach rechts aufgebaut:
PC1, PC2 so wie PC3 ist via Straight-Through-Kabel mit dem LAN - Switch verbunden.
PC1 hängt an Switch Interface FA 0/1, PC2 an Switch Interface FA 0/2 und PC3 an Switch Interface FA 0/3.
PC1 gehört zu VLAN 10 mit dem Netzbereich 192.168.10.0 bis 192.168.10.255/24.
PC2 gehört zu VLAN 20 mit dem Netzbereich 192.168.20.0 bis 192.168.20.255/24.
PC3 gehört zu VLAN 30 mit dem Netzbereich 192.168.30.0 bis 192.168.30.255/24.
Vom Interface FA 0/24 ist der Switch via Straight-Through-Kabel an das LAN - Router Interface FA 0/0 angeschlossen. Diese Verbindung ist zeitgleich der VLAN Trunk.
Es folgt der DMZ-Bereich welcher aus drei weiteren Elementen besteht:
Dem DMZ – Switch, DMZ – Server und DMZ – Router.
Der DMZ – Bereich regelt zum einen den Zugriff auf öffentliche Dienste und schützt zeitgleich das interne Netz vor nicht autorisiertem Zugriff von außen.
Über Interface FA 0/1 ist der Switch mit dem LAN - Router , über Interface FA 0/ 3 mit dem DMZ - Server und über FA 0/2 mit dem DMZ - Router verbunden.
Der DMZ – Router ist außerdem noch über Interface FA 0/1 mit der Internet Cloud via Telefonkabel verbunden.

Versuchsdurchführung

RADIUS steht für **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice und ist ein Sicherheitsprotokoll zur Identitätsprüfung und zur Überprüfung der Netzzugriffsberechtigung zwischen Client und Server.
RADIUS ist ein Teil des AAA Sicherheitskonzeptes.
Ziel dieses Versuches ist es, den LAN und den DMZ Router für die Authentifizierung mit RADIUS zu konfigurieren.
Außerdem werden beide Router für die SSH Fernsteuerung eingestellt.

AAA und Radius Konfiguration der Router

```
Router> enable
Router# conf t
Router(config)# aaa new-model
(Aktiviert AAA.)
Router(config)# aaa authentication login default group radius local
(Um einem Serverausfall entgegen zu Wirken, wird zusätzlich als Lokales
Backup, der Standard Benutzername und das Passwort geändert.)
Router(config)# username backuplocal privilege 15 secret backuplocal
Router(config)# radius-server host 204.204.7.3
(Die IP-Adresse unter der, der AAA – Server erreichbar ist.)
Router(config)# radius-server key pwradius
(Globaler Schlüssel zum entschlüsseln.)
Router(config)# line vty 0 4
Router(config-line)# login authentication default
Router(config-line)# exit
Router(config)# line console 0
Router(config-line)# login authentication default
Router(config-line)# exit
```

SSH Konfiguration der Router

SSH ist die Abkürzung für **S**ecure **S**hell und ist ein Protokoll, welches eine sichere Verbindung mit einem entfernten Gerät herstellt.
Im Vergleich zu Telnet, ist SSH die sicherere Variante, da der Benutzername, sowie das Passwort verschlüsselt werden.
Verschlüsselt wird mit dem RSA-Kryptosystem, dabei wird ein öffentlicher und ein privater Schlüssel erzeugt. Der private Schlüssel wird gebraucht um Daten zu entschlüsseln und der öffentliche Schlüssel, um Daten zu verschlüsseln.

```
Router> enable
Router# conf t
Router(config)# ip domain-name company.com
(Domain Name wird gesetzt, damit der RSA – Schlüssel generiert werden
kann.)
Router(config)# line vty 0 4
Router(config-line)# transport input ssh
Router(config-line)# exit
Router(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
(1024 bit RSA – Schlüssel wird generiert.)
```

Versuchsergebnisse

Die Router wurden soweit Konfiguriert und der AAA-Service auf dem Server aktiviert.
Wenn nun ein Client z.B. auf einen Dienst zugreifen möchte, welcher von dem Server angeboten wird, durchläuft der Client die drei A´s. Der Server überprüft die Eingabe, lehnt die Anfrage ab bei nicht Übereinstimmung , oder gibt die Freigabe zur Nutzung.
Des weiteren wurde dafür gesorgt das die Übertragung des Benutzernamens sowie des Passwortes verschlüsselt übertragen wird mit Hilfe des SSH - Protokolls und durch dritte nicht einsehbar ist.

Quellenverzeichnis

http://www.aulis.hs-bremen.de/goto.php?target=file_575645_download&client_id=hsbremen
20.10.2015

http://www.elektronik-kompendium.de/sites/net/0906151.html
20.10.2015

http://www.aulis.hs-bremen.de/goto.php?target=file_568275_download&client_id=hsbremen
20.10.2015

Abbildungsverzeichnis

Abb. 1 http://windowsitpro.com/site-files/windowsitpro.com/files/archive/windowsitpro.com/content/content/39744/napt.gif
20.10.2015