Тема бр.5 Контрола на пристап на мрежата и пресметување во облак

5.1 Дајте кратка дефиниција за контрола на пристап до мрежата.

• Термин за управување со пристап до мрежа; врши автентикација на корисниците кои се најавуваат во мрежата и одредува до кои податоци можат да пристапат и активности што можат да ги извршат
• Исто така, го испитува и здравјето на компјутерот или мобилниот уред на корисникот
NAC системите се занимаваат со три категории на компоненти:
Барател за пристап (Access Requester - AR)
• Јазол што се обидува да пристапи до мрежата и може да биде кој било уред со кој управува NAC системот, вклучувајќи работни станици, сервери, печатари, фотоапарати и други уреди со можност за IP (исто така се нарекуваат баратели или клиенти)
Сервер за полиси (Policy server)
• Одредува каков пристап треба да се даде
• Често се потпира на позадинските системи, антивирусни програми, управување со верзии или директориуми, за да се утврди состојбата на домаќинот.
Сервер за мрежен пристап (Network Access Server - NAS)
• Функционира како точка за контрола на пристап за корисниците на оддалечени локации што се поврзуваат со внатрешната мрежа на претпријатието/фирмата
• Може да има свои сервиси за автентикација или да се потпира на посебна услуга за автентикација од серверот за полиси

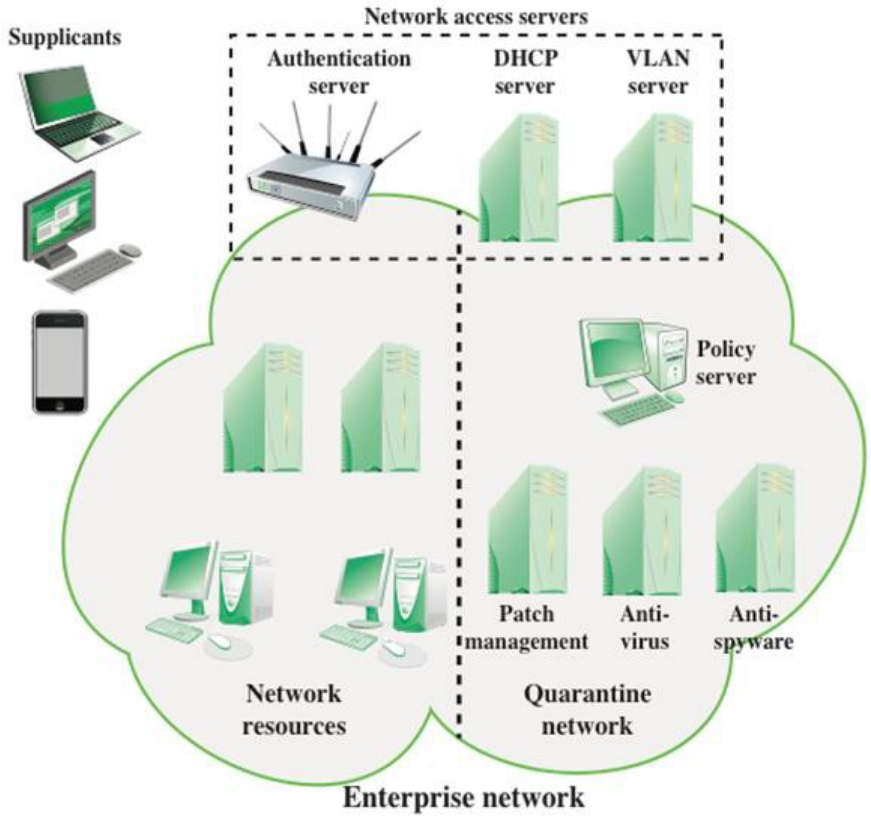

Figure 5.1 Network Access Control Context

1. Различни клиенти (AR) бараат пристап до мрежа на претпријатија со примена на некој вид NAS. Првиот чекор е генерално да се автентицира AR.
• Автентикацијата може да ја изврши NAS, или NAS може да посредува во постапката за автентикација (преку сервер за полиси).
• Го верификува идентитетот на подносителот на барањето кој што потврдува дека е негово
2.Серверот за полиси или серверот за поддршка вршат проверки на AR за да утврдат дали треба да му се дозволи интерактивна конекција за далечински пристап.
• Овие проверки - понекогаш наречени здравствени, бараат од софтверот на системот на корисникот да потврди усогласеност со одредени барања од основната конфигурација на организацијата
• На пример, antimalware софтверот на корисникот мора да биде ажуриран, оперативниот систем мора да биде целосно заштитен (patched), а оддалечениот компјутер мора да биде во сопственост и контролиран од организацијата.
• Врз основа на резултатите од овие проверки, организацијата може да утврди дали на далечинскиот компјутер треба да му биде дозволено да користи интерактивен далечински пристап.
• Ако корисникот има прифатливи овластувања за овластување, но оддалечениот компјутер не ја помине здравствената проверка, на корисникот и на далечинскиот компјутер треба да му биде одземен мрежен пристап или да има ограничен пристап до т.н. карантинска мрежа за да може овластениот персонал да ги отстрани безбедносните недостатоци.
3.Откако AR е автентициран и има одредено ниво на пристап до мрежата на претпријатието, NAS може да му овозможи на AR да комуницира со ресурсите во мрежата на претпријатието.
• NAS може да посредува во секоја размена за спроведување на безбедносна политика за овој AR, или може да користи други методи за ограничување на привилегиите на AR.

5.2 Што е EAP (Extensible Authentication Protocol)?

• EAP обезбедува услуга за транспорт за размена на информации за автентикација помеѓу систем на клиенти и сервер за автентикација
• Основната услуга за транспорт на EAP е проширена со употреба на специфичен протокол за автентикација, инсталиран и во EAP клиентот и во серверот за автентикација

5.3 Наведете ги и накратко дефинирајте четири методи за автентикација на EAP.

•EAP Transport Layer Security
-EAP-TLS (RFC 5216) дефинира како TLS протоколот (опишан во Поглавје 6) може да се вклучи во EAP пораките.
•EAP Tunneled TLS
- Слично на EAP-TLS, освен тоа што само серверот има сертификат со кој најпрвин се автентицира на клиентот. Серверот потоа може да ја користи воспоставената безбедна врска („тунел“) за да се автентицира клиентот.
•EAP Generalized Pre-Shared Key
-EAP-GPSK, дефиниран во RFC 5433, е EAP метод за взаемна автентикација и правење на сесиски клуч со употреба на претходно споделен клуч (PSK).
•EAP-IKEv2
-Дефинирана во RFC 5106; заснована на Internet Key Exchange protocol version 2 (IKEv2); Поддржува взаемна автентикација и воспоставување сесии со клучеви со користење на различни методи.

5.4 Што е EAPOL?

Основниот елемент дефиниран во 802.1X е протокол познат како EAPOL (EAP преку LAN).

• EAPOL работи во мрежните слоеви и користи на IEEE 802 LAN, како што е Етернет или Wi-Fi, на link ниво.

• EAPOL му овозможува на клиентот да комуницира со автентикатор и ја поддржува размената на EAP пакетите за автентикација.

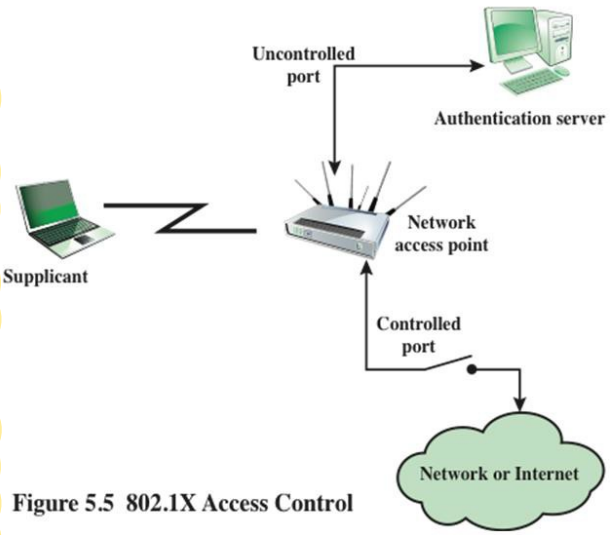

Figure 5.5 802.1X Access Control

• Кога подносителот на барањето најпрво ќе се поврзе со LAN, не ја знае MAC адресата на автентикаторот. Со испраќање на пакетот EAPOL-Start на специјална адреса за групен мултикаст резервирана за IEEE 802.1X автентикатори, подносителот на барањето може да утврди дали е постои таков автентикатор и да му каже на истиот дека барателот е подготвен.

• Во многу случаи, автентикаторот веќе ќе биде известен дека новиот уред е поврзан од известување за хардвер. На пример, hub ќе знае дека кабелот е вклучен пред уредот да испрати какви било податоци. Во овој случај, автентикаторот може да ја активира пораката за започнување со своја порака.

• И во двата случаи, автентикаторот испраќа порака за EAP Request Identity, енкапсулирана во пакетот EAPOL-EAP.

• EAPOL EAP е тип EAPOL рамка што се користи за транспорт на EAP пакети.

• Автентикаторот го користи пакетот EAP-Key за да испрати криптографски клучеви до барателот откако ќе одлучи да го прифати во мрежата.

• Типот на пакет EAP-Logoff означува дека подносителот на барањето сака да биде исклучен од мрежата.

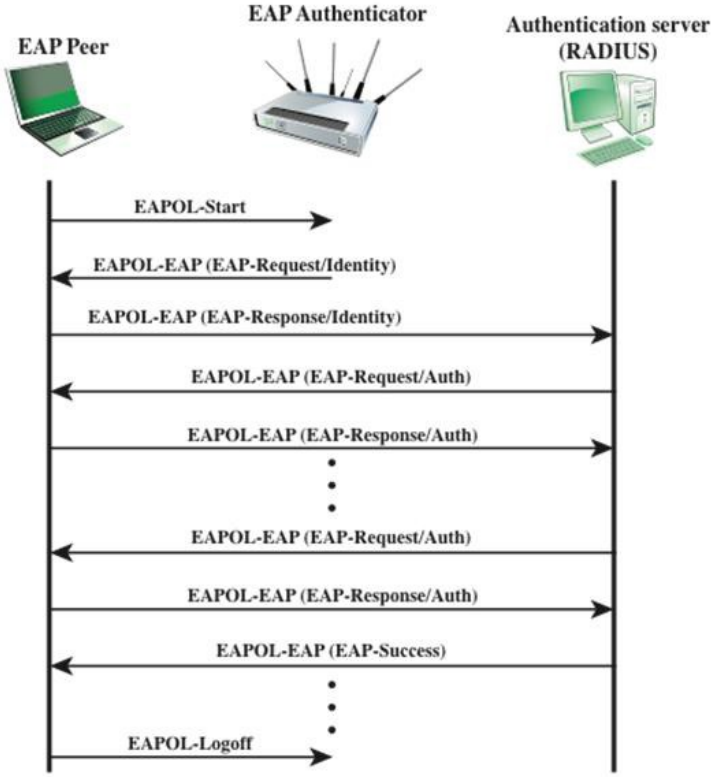

Figure 5.6 Example Timing Diagram for IEEE 802.1X

5.5 Koja e функцијата на IEEE 802.1X?

• Контролата на пристап до мрежа врз основа на порти IEEE 802.1X е дизајнирана да обезбеди функции за контрола на пристапот за LAN.
• Додека AS не го автентицира подносителот на барањето (со користење на протокол за автентикација), автентикаторот испраќа само пораки за контрола и автентикација помеѓу барателот и AS; Контролниот канал 802.1X е деблокиран, но каналот за податоци 802.11 е блокиран.
• Откако барателот ќе биде автентициран и ќе се обезбедат клучеви, автентикаторот може да пренасочува податоци од подносителот на барањето; под овие околности, каналот за податоци е деблокиран.

5.6 Дефинирајте што е пресметување во облак.

Модел за овозможување сеприсутен, удобен мрежен пристап до заедничка група на ресурси што можат да се конфигурираат (на пр. Мрежи, сервери, складирање, апликации и услуги) кои можат брзо да се обезбедат и да се ослободат со минимален напор за управување. Ваквиот облак модел промовира достапност и е составен од пет основни карактеристики, три модели на услуги и четири модели на deployment .

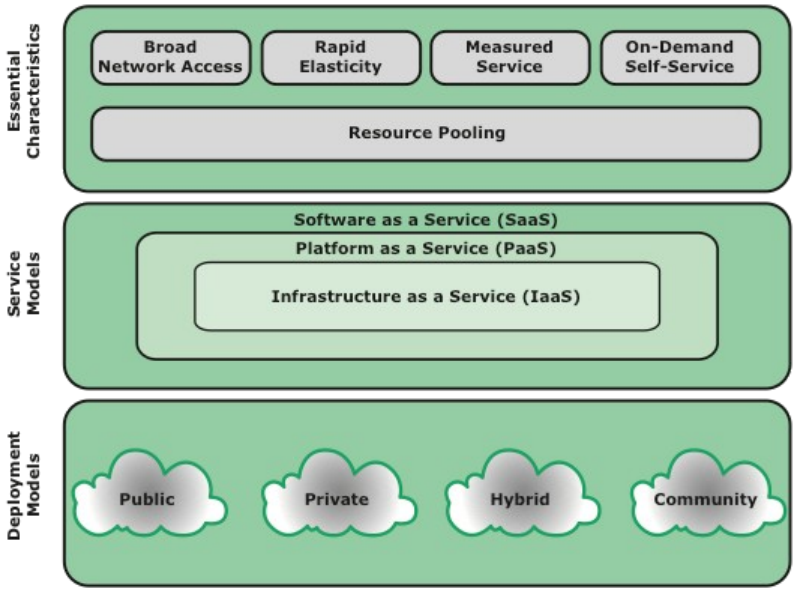

Figure 5.7 Cloud Computing Elements

5.7 Наведете ги и накратко дефинирајте три модели на услуга на облак.

- Софтвер како услуга (Saas): Способноста што му е дадена на потрошувачот е да ги користи апликациите на давателот на услуги кои работат на облачна инфраструктура. Апликациите се достапни од различни уреди со клиенти преку тенок клиентски интерфејс, како што е веб-прелистувач. Наместо да добие лиценца за работна површина и сервер за софтверски производи што ги користи, едно претпријатие ги добива истите функции од услугата cloud. SaaS ја зачувува комплексноста на инсталирање, одржување, надградба и закрпи на софтвер.
• Платформа како услуга (PaaS): PaaS често обезбедува услуги во стилот на Middleware, како што се база на податоци и услуги за компоненти за употреба од апликации. Всушност, PaaS е оперативен систем во облакот.
• Инфраструктура како услуга (IaaS): Способноста што му е дадена на потрошувачот е да обезбеди обработка, складирање, мрежи и други основни компјутерски ресурси каде потрошувачот е во состојба да распореди и да управува произволен софтвер, кој може да вклучува оперативни системи и апликации. IaaS им овозможува на клиентите да комбинираат основни компјутерски услуги, како што се складирање на податоци, за да градат високо адаптибилни компјутерски системи.

Platform Type	Common Examples
SaaS	Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting
PaaS	AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift
IaaS	DigitalOcean, Linode, Rackspace, Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)

5.8 Која е референтната архитектура за компјутерски облак?

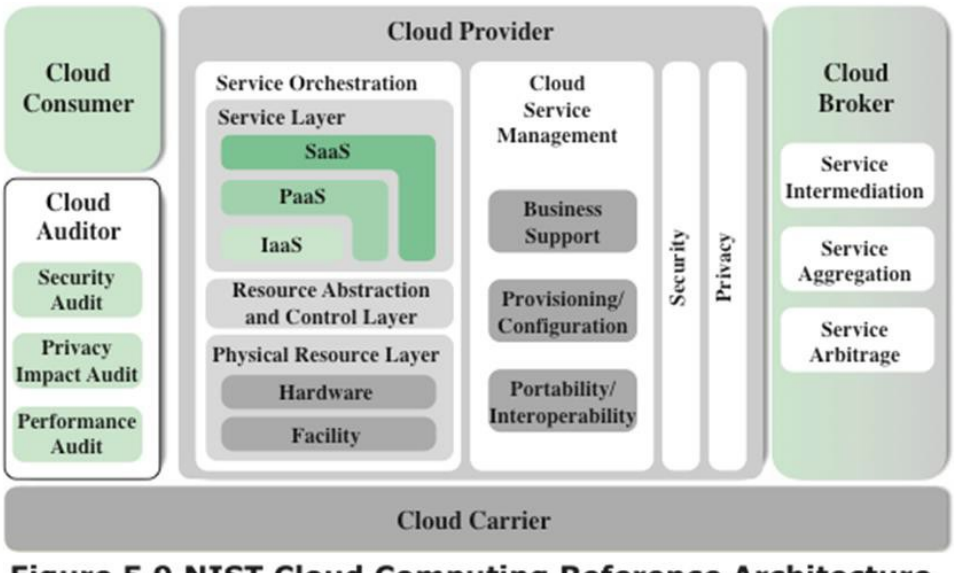

Figure 5.9 NIST Cloud Computing Reference Architecture

• Потрошувач во облак: Едно лице или организација што одржува деловен однос и користи услуги од провајдери на облак.
• Снабдувач на облак (CP): Лице, организација или субјект одговорен за достапноста на услугата за заинтересираните страни
• Cloud auditor: Страна што може да спроведе независна проценка на услугите на облак, работењето на информацискиот систем, перформансите и безбедноста на имплементацијата на облак.
• Cloud broker: Ентитет кој управува со употреба, перформанси и испорака на cloud услуги и преговара за односите помеѓу CP и потрошувачите на облак.
• Носач на облак: посредник кој обезбедува поврзаност и транспорт на услуги од облак од CP до потрошувачи на облак.

5.9. Опиши ја енкрипцијата на база на податоци во облак

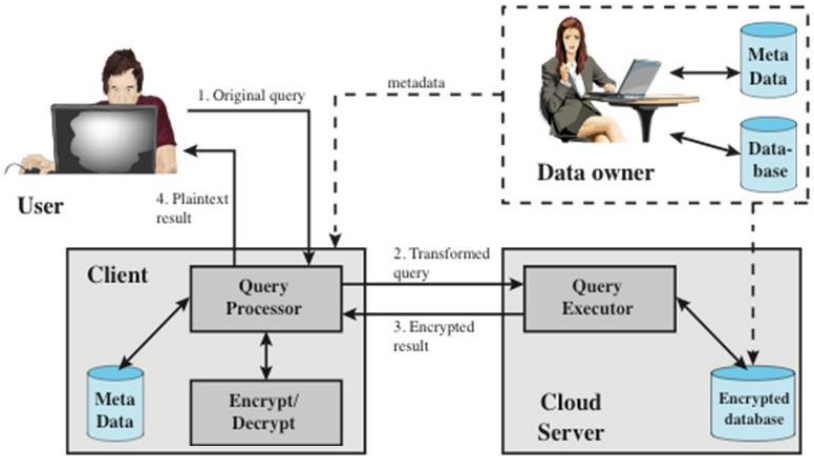

Figure 5.10 An Encryption Scheme for a Cloud-Based Database

1.Оригиналното query, од корисникот до процесорот за пребарување на query на клиентот, кој комуницира со метаподатоци на клиентот и криптирање / декрипција.
2.Трансформирано барање од процесор за пребарување на клиентот до извршител на барањето за облак-сервер, кој комуницира со криптираната база на податоци од облак. Шифрираната база на податоци вклучува метаподатоци и комуникација со базата на податоци со сопственикот на податоците.
3.Енкриптиран резултат од извршителот на барањето до процесорот за пребарување.
4.Plaintext резултат од пребарувањето до корисник.

Вклучени се четири субјекти:

• Сопственик на податоци: Организација која произведува податоци што ќе бидат достапни за контролиран пристап или во рамките на организацијата или на надворешните корисници.
• Корисник: Човечки субјект што доставува барања (прашања) до системот. Корисникот може да биде вработен во организацијата на која му е овозможен пристап до базата на податоци преку серверот, или корисник надворешен од организацијата на која, по автентикација, му се дозволува пристап.
• Клиент: Frontend што ги трансформира барањата од корисникот во прашања за шифрираните податоци зачувани на серверот.
• Сервер: Организација што ги прима шифрираните податоци од сопственикот на податоците и ги прави достапни за дистрибуција на клиенти. Серверот всушност може да биде во сопственост на сопственикот на податоците, но, обично е објект во сопственост и одржуван од надворешен провајдер. (cloud систем)