Тема 22. Отдалечен достъп – възможности и принцип на работа

Какви услуги предлага отдалеченият достъп?
Кои потребители се нуждаят от отдалечен достъп?
Възможност за отдалечен достъп
Сигурност при отдалечения достъп
  Авторизация чрез парола
  Авторизация чрез ключове
  Ограничаване на достъпа до IP адреси
  Ограничаване на времето за достъп
  Заключване на акаунт
Въпроси

Целта на отдалечения достъп е да се свържем отдалечено към ресурсите в една локална или корпоративна мрежа. В близкото минало основен инструмент за това беше комутируемия (dial-up) достъп – през аналогов модем или ISDN – да се свърже мобилния компютър към локалната мрежа. Разрастването на Интернет, увеличаване на пропускателната способност направиха ненужен комутируемия достъп. Интернет се предлага в хотелите, аерогарите, бензиностанциите и на много други места. GSM операторите предлагат свързване към Интернет от всяко място, на което имат покритие. Интернет стигна до всеки офис, до всеки дом.

Какви услуги предлага отдалеченият достъп?

1. *Свързаност към локалната мрежа*
   Съществуват протоколи за VPN – виртуални частни мрежи – които позволяват сигурно свързване на различни LAN в единна мрежа. Използват се т.нар. тунелни протоколи, информацията се криптира за гарантиране на сигурността на данните.
2. *Обмен на файлове*
   Дава възможност за достъп до файловете на отдалечен компютър чрез файлов трансфер. Много продукти предлагат възможност за синхронизиране на съдържанието на директория – анализират дали в локалната или в отдалечената система файлът е променен по-късно и предлагат копиране на новите и променени файлове.
3. *Терминален достъп*
   Позволява достъп до работния плот (desktop) на отдалечения компютър. Потребителят работи на отдалечения компютър, стартира програми, използва данни по същия начин, както при локален достъп до компютъра. Потребителят може да работи с големи обеми от данни. Тези данни се намират на контролираната машина и не се пренасят през мрежата. Обменя се само информация за промененатa област от екрана, за движението на мишката и клавиатурата.
   Тъй като потребителят работи на отдалечения компютър, той има достъп до неговите ресурси – дискови устройства и принтери. За пълноценна работа е необходимо използване и на печат. Продуктите за терминален достъп предлагат възможност за пренасочване на принтерите. Това позволява отдалеченият потребител да използва локалния си принтер за печат на документи.
4. *Достъп до сървъри за бази данни*
   Много от съвременните бизнес приложения използват SQL бази данни. Те генерират значително по-малък трафик в сравнение с традиционните файлово-ориентирани бази данни. Това позволява използването на приложенията със SQL бази данни от отдалечени компютри.

Кои потребители се нуждаят от отдалечен достъп?

1. Отдалеченият достъп е възможност за свързване на малки офиси с един до няколко компютъра към централизирана база от данни, използвайки интернет връзка.

2. Осигуряване възможност на служителите за дистанционен достъп до работните си места. Това позволява те да работят в извън работно време и дори да работят от дома си без да имат работно място в офиса.
3. Възможност на служители, които пътуват, да работят върху документи, намиращи се на работните им места или на сървъра.
4. Възможност за квалифицирана помощ от страна на компютърните специалисти на работните места на служители – позволява обучение, консултации, решаване на проблеми от специалиста отдалечено.

Възможност за отдалечен достъп

Основна среда за отдалечен достъп е Интернет. За да се осъществи доспъп до услуга, предоставена от компютър, е необходимо той да притежава реален IP адрес. Въведената политика за сигурност – за филтриране на трафика – трябва да позволява порта, използван от приложението, да бъде достъпен за външни потребители. Много компютри използват NAT за свързване към Интернет. Те имат IP адрес от частното адресно пространство и не са 'видими' от Интернет. Реален адрес има NAT рутерът. Рутерите притежават функционалност, която позволява пренасочване на портове – заявките получени към реалния IP адрес на зададения порт се пренасочват към компютър в локалната мрежа на зададен локален порт. За отдалечените компютри този процес е прозрачен – те използват услугата на зададен адрес и порт, така както ако компютърът предлагащ услугата притежава реален адрес.

Ако пренасочването не може да се изпълни е възможно използване на VPN. Съществуват безплатни и комерсиални услуги за такива клиенти. При тях сървър в Интернет приема техния входен и изходен трафик и го пренасочва към друг компютър във VPN.

Сигурност при отдалечения достъп

Отдалечената връзка представлява врата към външния свят, от която могат да се възползват и 'нежелани гости'. Отдалеченият достъп е риск в компютърната сигурност Спазването на политиките за сигурност ограничава възможностите за нерегламентиран достъп.

Авторизация чрез парола

Основният метод на авторизация е с потребителско име и парола. Спазването на политиката за използваните пароли при отдалечен достъп е изключително важно. Колкото е по-сложна паролата, толкова вероятността за нейното отгатване намалява.

Съвременните компютърни системи не съхраняват паролите за достъп. Вместо това те използват алгоритми за хеширане – създава се цифрова стойност – ключ, която отговаря на използваната парола. Ако злонамерен потребител знае хеш ключа, той ще се опита да намери парола, която отговаря на този ключ. Може да използва няколко стратегии: 1 – използване на лична информация: имена на роднини, домашни животни и дати; 2 – използване на думи от речник, атакуващият създава на всички думи от речника хеш ключове, ако използваната парола се съдържа в речника, то съответствието се намира веднага; 3 – метод на грубата сила (brut force) – изчисляват се хеш функциите за всички възможни ключове. Това е опит за разгадаване на паролата. Колкото по-кратка е тя, толкова по-малко време е необходимо за нейното разбиване.

Затова, приетата политика за сигурност обикновено включва следните правила:

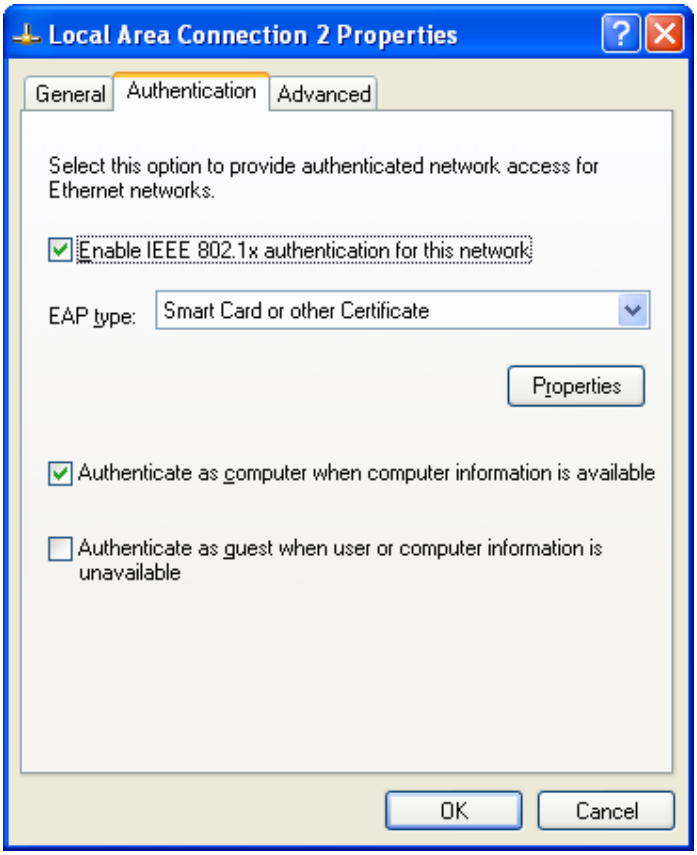
1. Не се използват за пароли лични данни;
2. Не се използват думи, които мога да се намерят в речник – използването на дума с допусната правописна грешка е добра идея;
3. Да не се използват къси пароли. Обикновено дължина от 8-10 символа в момента се счита за достатъчна. Паролата е необходимо да съдържа – поне една голяма буква, поне една малка буква, поне една цифра. Това увеличава броят на възможностите и прави неприложим метода на грубата сила за отгатване на паролата.
4. Паролите да се променят периодично. Колкото по-дълго се използва една парола, вероятността за нейното компрометиране нараства.

За авторизация с парола се използват протоколите PAP (Password Authentication Protocol) и CHAP (Challenge Handshake Authentication Protocol). CHAP използва криптиране на паролите.

Авторизация чрез ключове

Протоколът за авторизация EAP (Extensible Authentication Protocol) позволява авторизация чрез ключове – PSK (pre-shared keys) и използване на система с публичен ключ PKI (Public Key Infrastructure). Използването на PKI – сертификат, публичен и частен ключ съхранени върху смарт карта гарантира най-високо ниво на сигурност.

Забележка: Windows поддържа EAP. В настройките на мрежовата карта има страница с име: 'Authentication':



Фиг. 22-1. Включване на авторизация

Ограничаване на достъпа до IP адреси

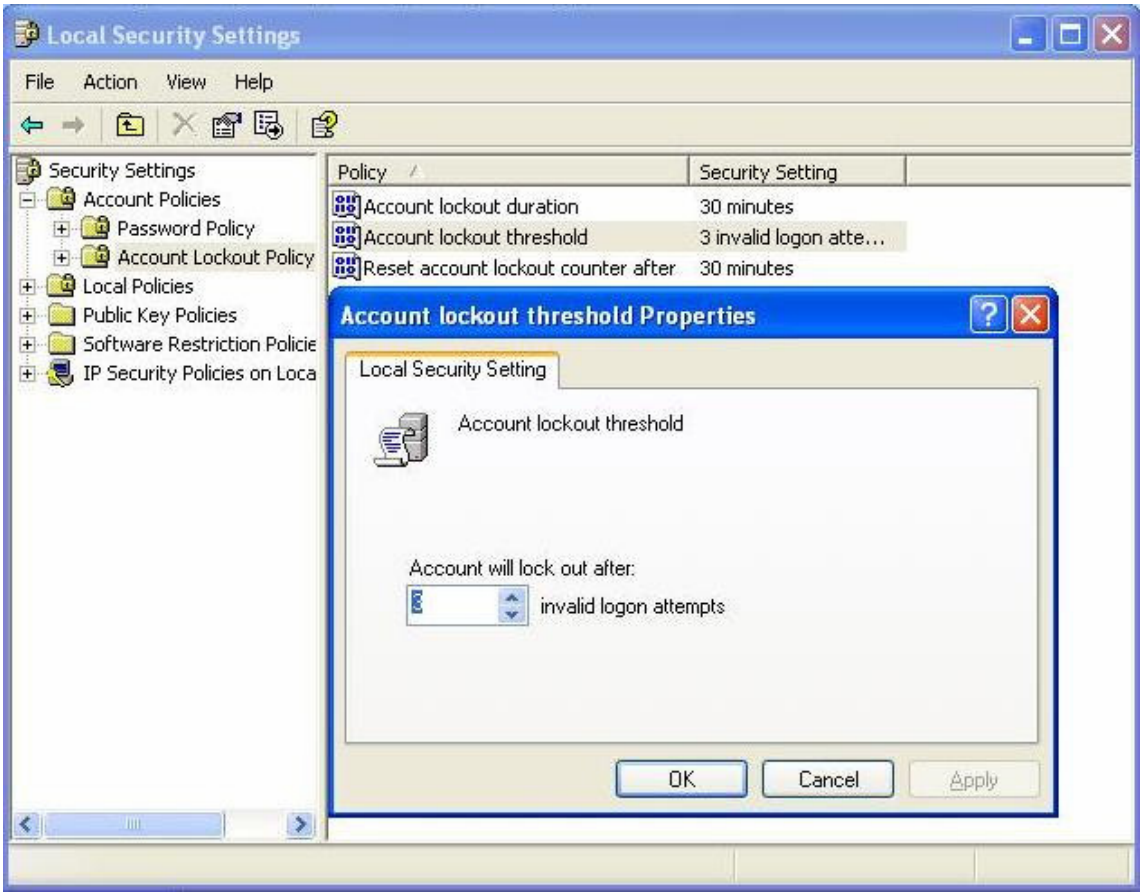
Ако отдалечените потребители използват фиксирани работни места е възможно да бъде конфигурирано използването на статичен реален IP адрес. Това позволява ограничаване на възможностите за използване на услугата за ограничен достъп, чрез настройване на защитната стена да пропуска услугата само за конкретен списък от адреси. Това значително намалява риска от неоторизиран достъп.

Ограничаване на времето за достъп

Може да се регламентира времето за отдалечен достъп за конкретни потребители – примерно в извънработно време. Може да се ограничи времето, през което потребителят е свързан отдалечено.

Заключване на акаунт

Заключването на акаунт е политика, при която след определен брой неуспешни опити потребителят се блокира за определено време. В примера, след 3 неуспешни опита потребителите ще бъдат блокирани за 30 минути. Това пречи на неоторизираните потребители да познаят паролата.



Фиг. 22-2. Заключване на акаунт

Въпроси

1. Кои услуги можем да ползваме при отдалечения достъп?
2. Какви са възможностите за реализиране на отдалечен достъп?
3. Какви правила трябва да спазваме, за да се гарантира сигурността на системата при разрешен отдалечен достъп?