ВИРТУАЛНИ ЧАСТНИ МРЕЖИ

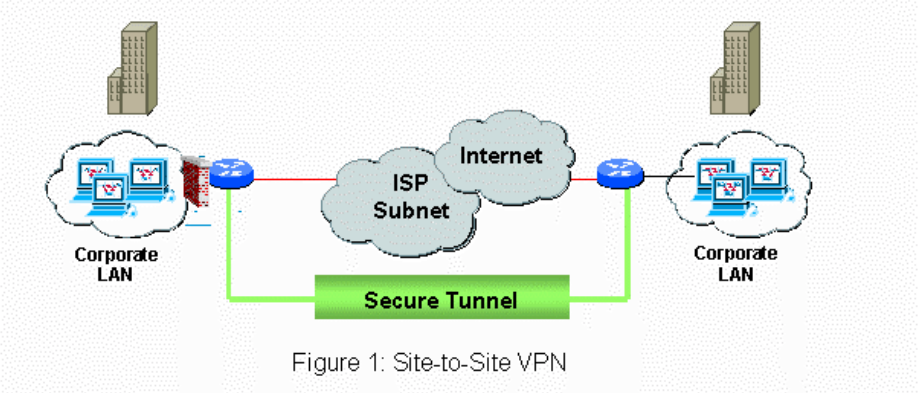

Figure 1: Site-to-Site VPN

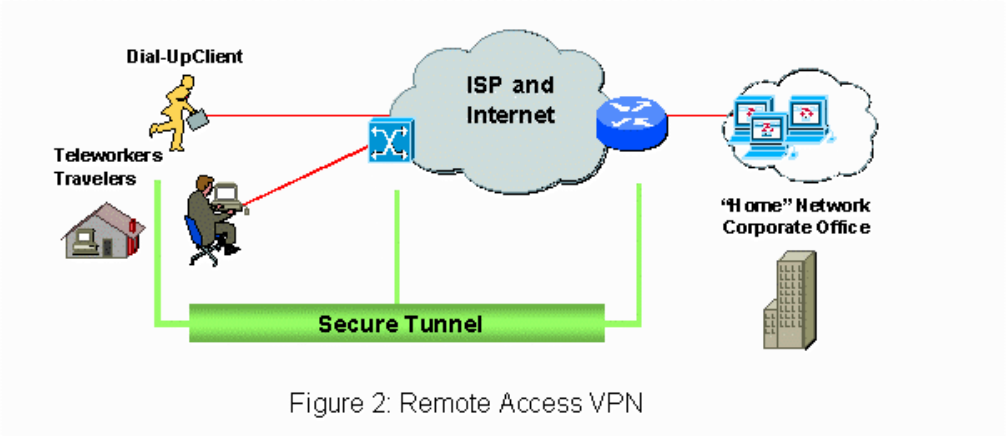

Figure 2: Remote Access VPN

Какво представлява VPN?

Обяснението на термина виртуална частна мрежа се състои в обяснението на трите съставящи го думи.

Мрежа

Мрежата представлява компютри, които комуникират един с друг.

Виртуална мрежа

В локалните (LAN) и глобалните (WAN) мрежи има мрежова преносна среда(), кабелна или безжична, която директно свързва комуникиращите компютри. Виртуалната мрежа не притежава такава среда, тя създава тунел през обществена мрежа, например Интернет, и двата комуникиращи компютъра се свързват към мрежата. Този вид връзка наподобява връзката”от точка до точка”() и това се постига, чрез капсулиране на данните.

Частна мрежа

Тъй като данните са криптирани, когато преминават през обществената мрежа, то те остават частни, не могат да бъдат прочетени от никой(освен, ако не разполага с ключа за криптиране).

Начин на работа

VPN може да се конфигурира да работи по dialup връзка или като връзка между два маршрутизатора. При врория тип връзка отговаряшият маршрутизатор има посветена Интернет връзка, а извикващият маршрутизатор използва dialup Интернет връзка.

Тунелиране

Тунелът, създаден в една VPN връзка, представлява логическа връзка от точка до точка, която представлява автентикация и криптиране на данни от едната крайна точка на тунела до другата.

Процес на капсулация

При тунелирането оргиналният пакет се скрива във вътрешността на нов пакет.За да се извърши маршрутизацията на пакета през тунела, адресът на крайната точка на тунела се задава във хедъра на новия пакет, който се нарича хедър на капсулацията. Адресът на крайното местоназначение се намира вътре в хедъра на оргиналния пакет. Когато хедъра достигне до крайната точка на тунела, хедъра на капсулацията се снема. Оргиналния пакет се доставя до крайното местоназначение.

Тунелиране от Слой 2 (Layer 2 of the OSI model)

VPN мрежите използват тунелни протоколи, които осигуряват виртуалната връзка от една точка до друга. Примери за такива протоколи са Point-to-Point Tunneling Protocol(PPTP), Layer2 Forwarding (L2F) Layer2 Tunneling Protocol.

Тунелиране от Слой 3(Layer 3 of the OSI model)

Тунелите изграждани в мрежовия слой осигуряват IP-базирани връзки. Тези връзки работят чрез изпращане на IP-пакети, капсулирани във вътрешността на специфицирани от Internet Engineering Task Force(IETF) протоколни обвивки. Обвивките използват IPSecurity(IPSec), Internet Key

Exchange(IKE) и методи за автентикация и криптиране, като Message Digest 5(MD5), Data Encryption Standard (DES) и Secure Hash Algoritym(SHA).

VPN ПРОТОКОЛИ

Във виртуалните частни мрежи се използват три типа протоколи:

-Тунелен протокол (VPN протокол)-използва се за изграждане на тунела.

-Протокол за криптиране (протокол за сигурност)-използва се за сигурност на данни.

-Мрежов/транспортен протокол (LAN протокол)-използва се за комуникация по частната мрежа.

Тунелни протоколи

Тунелните протоколи капсулират данните така, че хедърите на оргиналния протокол се обвиват вътре в капсулиращите хедъри.

PPTP

PPTP на Misrosoft е протокол от слой 2 за изграждане на WANs, изграден е на основата на Point-to-Point Protocol (PPP) и осигурява капсулирането и маршрутизацията на мрежови трафик през несигурна обществена мрежа (например Интернет). Начин на работа:

1. PPTP капсулира PPP фрейм, който може да бъде IP,IPX или NetBEUI пакет, във вътрешността на Generic Routing Encapsulation (GRE) хедър. Добавя се IP хедър за осигуряване на IP адресите на източника и на местоназначението. Адресът на източника е този на VPN клиента, а адресът на местоназначението е този на VPN сървара.
2. Данните в оргиналната диаграма обикновено са криптирани. VPN мрежите на Microsoft използват протокола MPPE заедно с PPTP за осигуряване на сигурни комуникации.

PPTP-linux е клиентски софтуер, който се изпълнява на Linux и Unix машини. Той им позволява да установят връзка към PPTP сървари. Софтуерър на PPTP сървъра (наречен PoPToP) е достъпен за Linux, Sun Solaris, FreeBSD и други реализации на Unix. Той поддържа Windows клиенти, както и PPTP-linux, и се разпространява като фрийуер.

Macintosh клиенти могат да се свържат към Windows PPTP сървари със софтуер на независими производители, като Network Telesystems TunnelBuilder.

L2F

Технологията L2F е разработена през 1996 от Cisco Systems и включва техния софтуер IOS. Като алтернатива на PPTP, L2F има възможност да използва ATM и Frame Relay протоколи за тунелиране. За разлика от PPTP, който изсква IP, за да работи L2F не изисква. L2F осигурява автентикация на крайните точки на тунела.

L2TP

L2TP протокола е резултат от сътрудничеството на Microsoft и Cisco, той е комбинация от възможностите на PPTP и L2F. L2TP капсулира данните за изпращане по IP(както прави PPTP), но може да ги капсулира и за изпращане по ATM, Frame Relay и X.25.

Предимства на L2TP пред PPTP:

-L2TP поддържа множество тунели между крайни точки. Това позволява създаване на множество тунели, които поддържат различно качество на услугата (QoS).
-L2TP поддържа компресиране на хедъри, което спестява допълнително информация.
- L2TP работи по не-IP интернетмрежи, използващи ATM или Frame Relay виртуални вериги.

IPSec

IPSec може да бъде използван за криптиране на данни, който текат през тунел изграден от друг протокол, например L2TP. Той може да бъде използван и за изграждане на тунел, когато действа в режим на тунелиране. В режима на тунелиране IPSec може да бъде конфигуриран за защита на данните между два IP адреса или между две IP подмрежи.
IPSec може да използва един или два протокола: Authentication Header (AH) и Encapsulation Security Payload(ESP).

AH тунелен режим

AH тунелен режим, използван сам по себе си, не осигурява криптиране на данните, които пътуват през тунела. Той верифицира, че данните не са пипани и автентицира изпращача. При AH не може да бъде направена никаква промяна на адреса на източника или местоназначението от момента, в който пакетът напусне началната точка на тунела.

ESP тунелен режим

При ESP тунелния режим адресите на първоначалния източник и карйното местоназначение се съдържа в оргиналния капсулиран IP хедър. Външният хедър обикновено съдържа адресите на шлюзовете.
ESP тунелът криптира данните с помоща на алгоритмите DES или 3DES.

Интероперативност на IPSec

Операционната система Windows 2000 включва вградена поддръжка на IPSec. IPSec е стандарт на IETF, който работи също с Linux, Unix, Macintosh и други операционни системи, поддържащи фамилията протоколи IP. IPSec автентикацията може да бъде направена по различни методи, като предварително споделени ключове, Kerberos и сертифициращи услуги.
FreeS/WAN за Linux представлява реализация на IPSec, която е с отворен сорс, и е достъпна за сваляне по Internet.

SSH/SSH2

Първоначално SSH е бил предназначен за осигуряване на сигурна алтернатива на Unix r командите, като rsh, rlogin, rcp. SSH2 се е развил като сигурен тунелен протокол, който може да се използва за създаване на VPN мрежа, работеща под Linux или Unix. Типът на VPN мрежата изградена с SSH2, се нарича VPN на ниво верига. При този вид VPN шлюзовете работят в сесийния слой на OSI модела. SSH клиентския софтуер е достъпен и за Windows.
SSH може да бъде инсталиран на защитна стена, а тунелът да бъде изграден от SSH клиент с dialup Интернет достъп до защитната стена. Защитната стена може да бъде конфигурирана да препраща трафика до

сървъра по вътрешната мрежа. Това е решение на VPN връзки, но с ниска производителност. SSH изисква акаунт за логване.

CIPE

CIPE представлява драйвер за ядрото на Linux, който може да бъде използван за осигуряване на сигурен тунел между две IP подмрежи. Данните се криптират в мрежовия слой на OSI модела. Това криптиране се нарича криптиране на ниско ниво. Предимството на този вид криптиране пред криптирането на високо ниво е, че при него не трябва да бъдат правени никакви промени на приложния софтуер, когато две мрежи се свързват с помоща на VPN. CIPE е по-прост и ефективен от IPSec.

Протоколи за криптиране

MPPE

MPPE се използва с PPTP-базирани VPN връзки(или PPP dialup връзки) и може да използва криптиращ алгоритъм с 40, 56 или 128-битов ключ.

IPSec криптиране

IPSec използва DES или 3DES за криптиране на данните в L2TP тунел.Използването на комбинация от криптографско -базирани алгоритми и ключове прави информацията много сигурна. Алгоритъмът на Дифи-Хелман позволява сигурен обмен на споделен ключ без изпращане на самия ключ по мрежата.

VPNd криптиране: Blowfish

VPNd за Linux използва криптиращ алгоритъм Blowfish. Това е 64-битов алгоритъм, който може да използва ключове с променлива дължина, от 32-бита до 448-бита. Той е бърз и неговия сорс код е достъпен. Съществуват няколко варианта GOLDFISH, DOSFISH и TWOFISH.

SSH криптиране

Unix SSH използва криптография с публичен ключ за криптиране на данните.

LAN протоколи

За да могат VPN клиентът и сървърът да комуникират, те трябва да имат общ стек от мрежови/транспортни протоколи. Това може да бъде TCP/IP, но не е задължително. Дори и при PPTP връзка, който изисква IP, частната мрежа може да използжа IPX/SPX или NetBEUI.

Приложение

Защо използваме VPN? В някои случаи dialup сървъра може да свърши същата работа, като VPN, но в други случаи VPN мрежата има предимства.

Сравнение между VPN и dialup

Предимства на виртуалните частни мрежи пред dialup достъпа:

- VPN мрежите спстяват разходит за мждуградските разговори, когато отдалечените потребители се намират изжън областта за набиране на локални номера.
- VPN мрежите изискват по-малко телефонни линии за осигуряване на отдалечен достъп до множество потребители едновременно.
- VPN мрежите изискват по-малко хардуерно оборудване, например банки от модеми.

- VPN мрежите, базирани на ISP, редуцират цените за адмнстриране и обучение.

Недостатъци на виртуалните частни мрежи пред dialup достъпа:

- VPN мрежите изискват и двата края на връзката да имат Интернет връзка. Това е проблем, ако един от двата края има ненадеждна Интернет връзка.
- Производителността при VPN мрежите често е по-ниска от тази при dialup връзката. Това зависи от типа на реализицията на VPN и от типа на Интернет връзките. Добавянето на VPN слой влияе на производителността до известна степен.

Сценарии на изграждане на VPN мрежи

- За осигуряване на отдалечен достъп до мобилни служители на компания или такива, които работят от вкъщи.
- За осигуряване на екстранет мрежа, до която да имат достъп служители, клиенти и партньори.
- За оцигуряване на връзка между два офиса в различни местоположения без за целта да се изгражда специална директна връзка.

VPN мрежи за отдалечен достъп

VPN клиентът трябва да може да използва протоколите, поддържани от VPN сървъра (тунелни, мрежови, транспортни и протоколите за криптиране). Установяване на връзка:

1. Домашният потребител набира локален ISP и влиза с потребителски акаунт, за да изгради Интернет връзка. (Ако потребителят има постоянна Интернет връзка тази стъпка не е необходима.)
2. Клиентът извиква сървъра за отдалечен достъп, конфигуриран да приема VPN връзки (използвайки IP адреса на отдалечения сървър); това действие изгражда тунела.
3. Потребителят се автентицира в частната мрежа и му се дава достъп.

Възможно е и домашен компютър да се конфигурира като VPN сървър и потребителят да се свързва към него от офиса за достъп до файлове съхранени не домашния компютър.

Виртуален Частен Екстранет

В този случай, част от LAN мрежата на организацията,наречена екстранет, се превръща в достъпна за отдалечени потребители по VPN връзка.

Важен проблем е защитата на останалата част от вътрешната мрежа от външен достъп. Поставянето на тази останала част от мрежата зад защитна стена може да даде сигурност.

Обикновено потребителите на екстранет осъществяват достъп до данни през Web браузър, затова в подмрежата с връзка към VPN се инсталира Web сървър. Също така там може да бъдат разположени и файлови сървъри.

Съществуващите и перспективни стандарти улесняват организациите

Да използват по екстранет общи данни и приложения, например групуер за разработване на проекти в сътрудничество. Тези перспективни стандарти са следните:

- Hypertext Markup Language (HTML)- Позволява споделянето на документи през всеки Web браузър. Потребителите не е нужно да имат конкретна програма за тексто обработка или друга програма, за да отварят файловете.
- Extensible Markup Language(XML) и Commerce XML(cXML)-Подобно на HTML, тези езици предлагат междуплатформена съвместимост.
- Open Buying on the Internet(OBI)- създава стандарти за тарнсакции на електронна търговия(e-commerce).

VPN връзки между филиални офиси

При създаване на VPN връзки между офиси на филиали се използва виртуална частна мрежа за свързване на два офиса във VPN конфигурация маршрутизатор-маршрутизатор (шлюз-шлюз). VPN сървърът може да действа като маршрутизатор с разширено IP препращане (foewarding). LAN мрежата във всеки офис има маршрутизирана връзка към Интернет. Тази връзка може да бъде набирана по необходимост или постоянна. При връзка с набиране при необходимост, маршрутизаторът, иницииращ връзката използва dialup Интернет връзка. Маршрутизаторът, който се извиква трябва да има постоянна Интернет връзка и трябва да бъде конфигуриран за приемане на връзки от вида набиране при необходимост. На извиквашия маршрутизатор се конфигурират две връзки с набиране при необходимост-едната за набиране на ISP и другата за свързване към VPN. Ако и двата маршрутизатора имат постоянни връзки към Интернет, VPN връзката може да бъде установена и оставена непрекъснато открита, ако е необходимо. VPN връзките от тип маршрутизатор-маршрутизатор могат да бъдат конфигурирани така, че единият маршрутизатор да действа като клиент и да инициира връзката, а другия да функционира като VPN сървър. Това е еднопосочна връзка. Двупосочната връзка е тази, при която всеки от маршрутизаторите може да инициира връзката. В този случай и двата маршрутизатора трябва да имат постоянна връзка към Интернет и трябва да бъдат построени като LAN и WAN маршрутизатори.

Може да бъде използван софтуер от сорта на vpnd(VPNdaemon) за свързване на две локални мрежи, използващи Linux и FreeBSD. За защита на данните преминаващи през връзката се използва алгоритъма Blowfish.

Типове VPN мрежи

Софтуерно-базирани VPN

Софтуерно-базираните VPN мрежи включват използването на тунелните протоколи. Тази категория може да бъде разделена допълнително на продукти на независими производители и VPN софтуер поддържан от операционната система. Предимството на последните е тяхната цена, тъй като не изискват допълнително заплащане и са достатъчни за нуждите на голяма част от организациите.

VPN софтуерните продукти на независимите производители обикновено предлагат долълнителни възможности и разширяват използваемостта на VPN, като често осигуряват повече опции за сигурност и в някои случаи по-

лесно реализиране. Някои софтуерно-базираните VPN мрежи позволяват да се предават данни в тунела на базата на протокола или IP адреса. Продуктите на независимите производители включват Safeguard VPN, Checkpoint SVN(Secure Virtual Networking) и NetMAX VPN Suite за Linux. Софтуерно VPN решение за Linux, което е безплатно, е FreeS/Wan, използва IPSec.

Хардуерно-базирани VPN

Хардуерно-базирани VPN мрежи се проивеждат от компании като Shiva, 3Com и VPNet Technologies, Cisco, IBM, Notrel. Поддръжката на VPN е вградена в маршрутизаторите на Cisco, както и в маршрутизаторите на други компании. NTS Tunnel-Builder осигурява сигурни VPN комуникации за Windows, NetWare и Macintosh. Такива производители като Raptor Systems предлагат VPN мрежи, базирани на такива защитни стени, които са компинирани със средства за сигурност.

Хардуерно-базираните VPN мрежи могат да се разделят на две групи:

- Базирани на маршрутизатори- Базираните на маршрутизатори VPN решения предствляват маршрутизатори с възможност за криптиране. Те предлагат по-добра производителност на мрежата и като цяло са по-лесни за инсталиране и използване.
- Базирани на защитна стена- Базираните на защитна стена VPN решения осигуряват допълнителни мерки за сигурност, силна автентикация и детайлно логване. Базираната VPN на защитна стена може също да извършва преобразуване на адреси. Производителността може да бъде проблем, макар че в някои реализации хардуерните криптиращи процесори решават този проблем.

Конфигуриране на VPN връзка

Конфигурирането на една VPN връзка зависи от типа на VPN и от това дали реализацията е хардуерна или софтуерна.

Инсталиране на VPN връзка в Windows 2000

Стъпка 1 Избира се Network and Dialup Connections от менюто Start.

Стъпка 2 Щраква се върху иконата Maka New Connection, за да се създаде VPN връзка.

Стъпка 3 Сега е стартиран съветника Network Connection Wizard. Избира се третата опция и така се свързваме към частната мрежа по Интернет.

Стъпка 4 След това трябва да се зададе следното:

- Дали да бъде избран сървър за установяване на първоначална връзка към Интернет- Ако изберем това ще трябва да конфигурираме или да изберем dialup връзка. Ако иамем постоянна Интернет връзка трябва да изберем “do not dial”.
- Името на хост или IP адрес на VPN сървъра- Въвеждаме информация за компътъра или маршрутизатора, към който искаме да изградим VPN връзка. Имената на хостовете се преобразуват в IP адреси, затова ако се въведе направо IP адреса ъе се намали сложността на връзката.

- Дали връзката трябва да бъде достъпна за всички потребители, които споделят компютъра, или само за потребителя, който я създава- По подразбиране е достъпно за вси4ки потребители да използват връзката.
- Дали да разрешим Internet Connection Sharing (ICS), за да споделяме VPN връзката по мрежата- Това позволява на други компютри в LAN да споделят връзката посредсвом Network Address Translation (NAT). IPSec не работи с NAT.

Стъпка 5

Въвеждане на името на връзката. Връзката е конфигурирана на компятъра на мрежата, за да се свъже към VPN мрежата се щраква двукратно върху иконата на връзката в Network and Dialup Connections и се въвеждат потребителско име и парола за отдалечения VPN сървър.

Windows 2000 създава връзката.

Използвайки подразбиращата се конфигурация (при тип VPN, зададен на Authomatic), софтуерът открива дали VPN сървърът използва PPTP или L2TP и след това използва подходящия протокол за изграждане на тунела. По всяко време може да се конфигърират или променят свойствата на връзката(например кои протоколи за автентикация трябва да бъдат използвани).

VPNs u Red Hat Linux

Red Hat Linux поддържа два метода за имлементиране на сигурна връзка, VPN и VPN-equivalent. Решението, което е близо до дефиницията на VPN е Crypto IP Encapsulation (CIPE), метод за свързване на две отдалечени локални мрежи така, че да функционират като една обща.

CIPE е VPN имплементация основно развита за Linux. CIPE използва криптирани IP пакети, които са капсулирани в дайтаграм UDP пакети. Пакетите носят информация за хедъра на изпрашача и са криптирани използвайки подразбирашия се алгоритъм за криптиране в CIPE. Тогава пакетите се трансферират върху IP като UDP пакети през CIPE виртуални мрежови устройства (cipcbx) през мрежовата преносна среда до желания отдалечен хост.

Инсталирането на CIPE е подобно на инсталирането на мрежов интерфейс под Linux. CIPE RPM пакет съдържа конфигуриращите файлове, намира се на /etc/cipe, CIPE daemon(/usr/sbin/ciped-cb), мрежови скриптове, които се качват(load) модула на кърнела и активират или дезактивират CIPE интерфейса (if*-cipcb), и примерни конфигурирани файлове, които се намират на /usr/share/doc/cipe-<version>/samples/. Има и подробно описание на CIPE протокола и различните подробности.

Инсталирането на CIPE между клиент и CIPE сървър дава възможност за сигурна “peer-to-peer” връзка използвайки Internet като среда за пренасяне на WAN трафика. Тогава клиента изпраща файл през Internet до CIPE защитната стена , където всеки пакет получава време на валидност(живот), криптира се и му се поставя адреса на съответната CIPE защитна стена на получателя. Тогава получаващото устройство прочита хедъра, отстранява го, изпраща пакета през отдалечения LAN маршрутизатор, за да бъде изпратен до получателя.

Сигурност на VPN

Сигурността на VPN има три компонента:

- Автентикация
- Авторизация
- Криптиране

Автентикация

Автентикацията на VPN клиента включва проверката за истинност на самоличността на машината и на потребителя, който инициира VPN връзката. Автентикацията мойе да бъде осъществена на нивото на машината. Например, когато една VPN връзка, базирана на Windows 2000, използва IPSec за L2TP VPN сертификатите на машините се обменят като част от изграждането на IPSec асоциация за сигурност.

Потребителят може да бъде автентициран с помоща на един от няколкото метода за автентикация, като Extensible Authentication Protocol (EAP), Challenge Handshake Authentication Protocol (CHAP), Shiva PAP(SPAP).

Авторизация

Авторизацията означава зададените ограничения, на базата на които на едни от потребителите се предоставя достъп до VPN, а на други се отказва.

Криптиране

За защита на данните във VPN мрежи могат да бъдат използвани най-различни технологии за криптиране. Много VPN реализации позволяват потребителя да избере метода за криптиране, който трябва да бъде използван. Криптирането осигурява сигурност на данни, които пътуват по VPN.

Сигурността на Windows NT 4.0-основани VPN

Windows NT 4.0 осигурява сигурност за VPN. Използва 40 или 128 битови ключове за криптиране и автоматично генерира ключ за всяка VPN сесия използвайки RC4 криптиращ алгоритъм.

Препоръчва се използването на 128 битови ключове тъй като разбиването на 40 битов ключ не е трудно.

Сигурността на PPTP

PPTP наследява сигурността на PPP. Осигурява на потребителя автентикация и защитава поверителността на клиентската информация. PPP се използва за транспортиране на информацията през PPTP тунела. PPP автентициращите методи използвани в Microsoft Windows 9x DUN Windows NT 4.0 RAS са Password Authentication Protocol (PAP), Shiva Password Authentication Protocol (SPAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), и Extensible Authentication Protocol (EAP) в Windows 2000. Microsoft Point to Point Encryption (MPPE) се поддържа в Windows 9x DUN и Windows NT 4.0 RAS. MPPE използва RC4 криптиращия алгоритъм.

PPTP зависи от два протокола да защитава информацията на потребителя на PPP ниво: MS-CHAP и MPPE. Най-новите реализации на PPTP и PPP поддържат MS-CHAP v2, която осигурява автентикацията ръчно, по-силни криптиращи ключове, разделя ключовете за криптиране на ключ за изпращане и ключ за получаване.

Типове атаки използвани срещу VPN

Атаките срещу VPN основно се разделят на 4 вида:

Impersonation-атаки, при които атакуващия се представя за друг човек. Методите за автентикация поддържани от PPTP могат да намалят ефективността на този тип атаки.

Integrity-атаки, при които информацията изпратена от потребителя се модифицира. Попринцип е невъзможно предпазването от този тип атаки, най-доброто, което може да се направи е да се разпознае модификацията. Електронните подписа са сащо защита срещу този тип атаки.

Disclosure-атаки в ресултат, на които информацията се получава от човек, за който не е предназначена. Вредата от този тип атака зависи от съдържанието на информацията. Защитата от този тип атаки е използването на силни криптографски алгоритми.

Отказ на услуга(Denial of service)- целта на тези атаки е да откажат услуга на валидни потребители. Практически невъзможно и най-трудно е предпазването от този тип атаки.

Атаки срещу PPTP и защити, подобрения на Misrosoft

Dictionary Attacks

Този тип атаки се състоят в това, че се използва голям списък от думи и чрез изпробване атакуващия се опитва открие парола. Криптираната парола се сравнява с всяка дума от списъка (също криптирана), докато се открие съвпадение. Всички видове автентикация използващи пароли са уязвими на този тип атака. LAN Manager authentication е особено уязвим. По тази причина не се поддържа в MS-CHAP v2. Използва се Windows NT метода за автентикация, който е по-устойчив на този тип атаки.

Server Spoofing

Тъй като се автентицира само PPTP клиента, възможно е фалшиф PPTP сървър да се представи за истинския. Фалшивият сървър може и да не успее да разкодира информацията, която изпраща клиента, но ще събере доста информация криптирана с един и същи ключ, което може да е полезно. Освен това, сървъра може да поиска от клиента да си смени паролата използвайки старата версия на MS-CHAP (CPW1). CPW1 е така проектиран, че фалшивият сървър може да притежава хеша на паролата на клиента и може да я използва, за да се представя с нея на истинския PPTP сървър или на RAS сървър.

В MS-CHAP v2 този проблем е отстранен автентикацията се прави ръчно(manual), което прави атаката по-трудна. Ръчно(manual) автентикация означава, че не само клиента се автентицира пред сървъра, но и сървъра се автентицира пред клиента.

Слаби криптиращи ключове

Криптиращите ключове използвани от MPPE се извличат от потребителската парола. Ако паролата е несигурна, то и ключа ъе бъде също толкова слаб.

Подобрението на Microsoft, което е включено в Windows NT 4.0 Service Pack 2, Service Pack 3, Service Pack 4 е че системата може да провери избора на

потребителя, дали паролата има минималната дължина и е случайна (не е дума от речник).

Повторна употреба на същия криптиращ ключ

Когато 40-битов криптиращ ключ е създаден, същият ключ за криптиране се използва във всички следващи PPTP сесии, докато потребителя не си смени паролата. Това е така, защото само паролата се използва за извличането на 40-битовия ключ, без друга допълнителна уникална информация за самата сесия. 128-битовия ключ няма този проблем, защото за неговото извличане се използва уникална за сесията информация. Както и да е, същият ключ се използва за двете изпращане и получаване на информация, което означава, че една и съща информация е криптирана с един и същи ключ всеки път.

В MS-CHAP v2 за извличането на 40 битовия и 128 битовия се използва уникална информация от сесията. В двете посоки (получаване и изпращане) се използват различни ключове.

Сингронизация на ключовете в MPPE

MPPE променя ключа за криптиране на всеки 256 пакета или когато се изгуби пакет.Ако получателя забелижи, че има липсжащ пакет, казва на изпращашия да промени ключа и да започне синхронизацията от начало. Това позволява на евентуален атакуващ да направи атака с отказ на услугата и да модифицира (брояча) времето на пакета или да предизвика ресинхронизация.

За да се избегне тази атака, в PPTP MPPE сменя ключа на всеки пакет.

PPP измами при уговарянето (Negotiation Spoofing)

PPP уговорките между PPTP клиента и сървъра са некриптирани и без автентикация. По тази причина, е възможно атакуващ да измами с PPP пакет, такъв който съдържа адреса на DNS сървъра или IP адрес, който да бъде използван от клиента. Може също така да бъде модифицирана информация в пакета.

Пасивно Наблюдение

Наблюдавайки PPTP контрола и каналите за информация по време на тунелирането различна информация за PPTP сървъра и клиента може да се получи.Тази информация включва IP адресите на клиента и на сървъра, вътрешния IP адрес на клиента на PPTP тунела, адресите на външните DNS сървъри дадени на клиента и потребителското име на клиента.

В MS-CHAP v2 са направени промени, които подобряват сигурността на PPTP протокола. Оснвния проблем остава, основно проблема с автентикацията и криптирането е, че те са толкова сигурни, колкото сигурна парола е избрал потребителя. Колкото по-бързи стават компютрите и атаките срещу пароли стават по осъществими и се достига до рабиване на паролите. Списъка с лоши пароли включва думи като: думи от речник, думи със случайно разместени букви, думи допълнени с числа, думи, в които букви са заместени с числа, обърнати думи, думи образувани от началните букви на други думи. Могат да се използват протоколи за автентикация и размяна на ключове, които не пзволяват да се прави dictionary атаки върху паролите на потребителите.

Сигурност на VPN създаден с IPSec

IPSec използва стандартния начин за за защита на данните с криптиращи алгритми, както и използването на ключове за автентикация.
IP Security Protocol, определя информацията, която трябва да се добави към IP пакета, за да се осигури поверителността, достоверността на информацията, определя как да бъде криптиран пакета.
IKE(Internet Key Exchange) е протокол управляващ размяната на ключове и се използва заедно с IPSec. Той осигурява на IPSec допълнителни предимства, гъвкавост и лесно конфигуриране. Осигурява сигурна комуникация на IPSec без да изисква допънително преконфигуриране и осигурява сигурна размяна на криптиращите ключове.
Проблемите, които може да се появят при използването на IPSec VPN зависят от имплементацията. Сигурността при използването на публични ключове зависи е толкова добра, колкото добър е механизъма за защита на частния ключ. Повечето IPSec имлементации поддържат сертифициране. Те генерират по-силни ключове от механизмите основани на генериране на ключ използвайки паролите. Пролема е, че някои имплементации на IPSec използват сертификати базирани на машината без едновременно с това да използват автентициране на потребителя. Ако клиентската машина се използва от повече от един човек, упълномощения достъп до мрежата основон на машиннен сертификат създава дупка във сигурността.
Предимствата на IPSec пред PPTP са, че не поддържа автентикация на ниво потребител (както паролите при PPTP) и използва автентикация с размяна ключове.

Сигурност на L2TP

Сигурността на L2TP зависи от имплементацията. Стандартно VPN изградена с L2TP използва IPSec, за да осигури защита на информаичта. При такива имплементации PPP автентикация обикновено се използва заедно с IPSec.

Сигурност на VPN при Linux

FreeS/Wan софтуерните VPN решения за Linux, които използват IPSec, действат като специализирани маршрутизатори, които установяват IP връзка между два потребителя. Когато пакета се изпрати от потребителя, той минава през маршрутизатора, който му добавя информация в хедъра за пътя, по който да мине и удостоверение (authentication) наречено Authentication Header(AH), и информация за CRC файловата цялост(коректност) и сигурност наречена Encapsulation Security Payload (ESP).
Имплементацията на IPSec прави FreeS/Wan сигурно решение. Изолзва се 3DES алгоритъма за криптиране и това защитава пакетите. При атака пакетите могат да бъдат отклонени, но прочитането на информацията е невъзможно(3DES използва 168-битов ключ). При “man-in-the-middle” атака между сървара и клиента атакуващия може да получи достъп и до ключовете разменяни по време на процеса на удостоверяване.
Има няколко причини поради, които CIPE е добър избор за сигурността:

- CIPE е достъпен на всички Red Hat Linux крайни машини(например, защитни стени), които искаме да свържем с Internet. Red Hat Linux също включва CIPE-поддържани криприращи ключове (шифари) в общата(основната) си дистрибуция.
- CIPE поддържа криптиране използвайки един от стандартните криптиращи алгоритми Blowfish или IDEA.
- Тъй като CIPE е софтуерно-базиран, някоя по-стара машина, на която може да се инсталира Red Hat Linux, може да се използва като CIPE гейтуей, така се спестяват средства за закупуването на допълнителни устройства за изграждането на VPN.
- CIPE е създаден да работи заедно с iptables, ipchains и други защитни стени основани на правила.
- CIPE конфигурирането се прави чрез текстов файл, позволявайки на администратора да конфигурира CIPE сървърите и клиентите отдалечено без да са необходими графични инструменти, който трудно могат да функционират по мрежата.

Съдържание

Използвани източници

Дж. Скамбрей, Ст. МакКлър, Дж.Къртс, “Защита от хакерски атаки”, СофтПрес, 2001
http://www.microsoft.com/NTServer/commserv/deployment/moreinfo/VPNSec_FAQ.asp
http://www.counterpane.com/pptpv2-paper.html
www.corecom.com/html/vpn.html
www.cisco.com