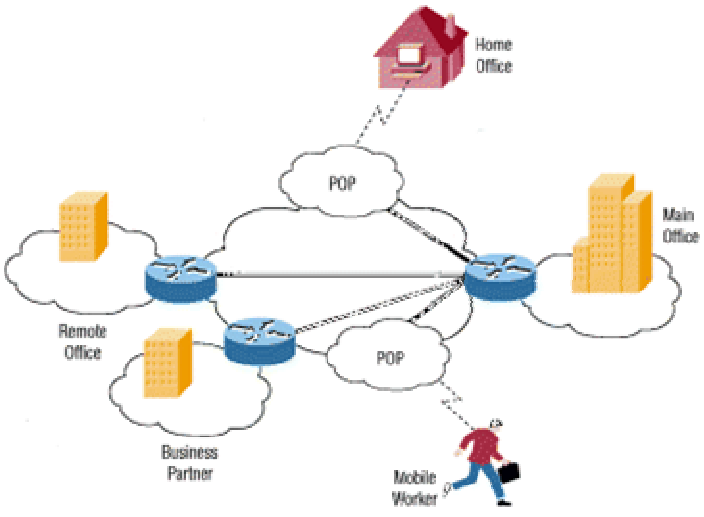
Проект

по Мрежова сигурност
на тема: Virtual Private Networks

изготвил: Йордан Илиев Шурелов
спец. Информатика, 3 курс, 5 група
ф.н. 43119

През последните десетилетия светът се е променил много. Много организации , вместо да работят само с местни компании, сега трябва да мислят по глобално.Много от тях са се разпространили по цялата страна или по света, и се нуждаят от бързи, сигурни и надеждни комуникации.
До скоро това означаваше използването на наети линии които да осъществяват WAN(wide area network).Наети линии вариращи от ISDN (integrated services digital network, 128 Kbps) до OC3 (Optical Carrier-3, 155 Mbps) позволяващи на компаниите да навлязат извън непосредствената си географска ширина.ЕднаWAN мрежа очевидно има предимства пред публична мрежа като Интернет когато говорим за надеждност, резултатност и сигурност.Но поддръжката на WAN особено използването на наети линии може да стане много скъпо и често цената расте с нарастването на разстоянието между обектите.
Първо се появи Intranet което всъщност е защитени с пароли участници за използване само от служителите на компаниите.Сега много компании осъществяват свои собствени VPN , за да осигурят нуждите на отдалечените офиси ислужители.



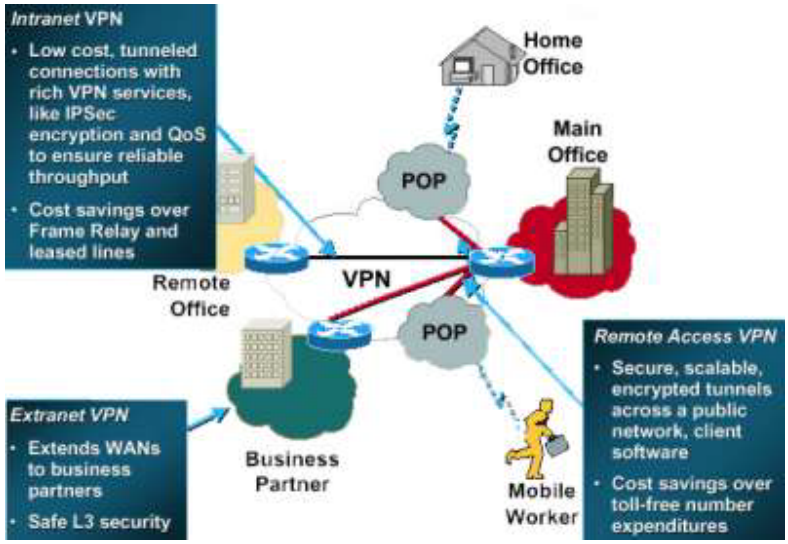
Една VPN връзка може да има една LAN в главната сграда на компанията, друга LAN в отдалечените офиси, и индивидуални юзъри.

VPN е частна мрежа, която използва публичната мрежа (обикновенно Интернет) , за да свърже отдалечените участници в комуникацията. Вместо използването на специална линия като наета например, VPN използва виртуална връзка през Интернет от локалната мрежа до отдалечения потрбител.

Има 2 вида VPN – Remote–access и Site-to-Site. Remote-access се нарича също VPND(virtual dial-up network), което е user-to-LAN връзка , използвана от компании които имат служители нуждаещи се от връзка до локалната мрежа от различни отдалечени места.Обикновенно , една корпорация която желае да настрои remote-access VPN ще се обърне до търговски доставчик (ESP – eneterprise service provider). Този ESP настройва network access server (NAS) и осигурява на отдалечените потребители desktop client софтуер за техните компютри. Участниците в комуникациите могат вече да се свържат с toll-free number за да достигнат NAS и да използват техния VPN client софтуер за достъп до мрежата на корпорацията. Един добър пример за компания която има нужда от remote-access VPN е голяма фирма с хиляди служители в сферата на продажбите.Remote-access VPN позволява сигурни криптирани връзки между вътрешната мрежа на компанията и отдалечените потребители чрез друг сървиз провайдър.

Site-to-site – Една компания може да свърже много части от своя бизнес чрез публична мрежа като

Интернет .Site-to-site VPN се разделя на Intranet-based и Extranet-based.
Inrtanet-based е когато една компания има едно или повече отдаличени места които те искат да вържат в single private network, те могат да открият intranet VPN за да свържат LAN с LAN.
Extranet-based е когато една компания има близки взаимоотношения с друга компания (партньор или клиент напр.) те могат да си построят една extranet VPN която свързва LAN с LAN , и това позволява на различните компании да работят в обща среда.
.



Пример за 2 -та вида VPN

Предимсвата на една VPN мрежа:

- Разширява географския обхват
- Подобрява сигурноста
- Редуцира разходите в сравнение с традиционната WAN
- Редуцира разходите за транспорт на отдаличените юзъри
- Подобрява продуктивноста
- Опростена мрежова топология
- Осигурява глобалнимрежови възможности
- Осигурява телекомуникационна поддръжка
- Осигурява по бързо връщане на инвестициите от традиционната WAN

VPN технологии

Основните моменти при разработката на VPN през Интернет с които трябва да се съобразяваме са **сигурност** и **продуктивност**. Transmission control protocol (TCP) IP и Интернет не са били съобразени с тези концепции при първоначалната им разработка, тъй като броя на потребителите и вида на приложенията първоначално не са изисквали голяма сигурност и добра продуктивност.

VPN се нуждае от следните 4 функции за да осигури силна защита на информацията:

- Authentication – доказване произхода на информацията
- Access control – ограничаване на достъпа на неауторизираните потребители
- Confidentiality – не всеки има право да чете или копира информация докато сърфира в Интернет
- Data integrity – никой не може да променя информацията при сърфирането си в Интернет

Различните password-based системи и challenge – response системи като challenge handshake authentication protocol (CHAP) и remote authentication dial-in service (RADIUS) – както и hardware – based автентикатори и дигиталните сертификати могат да бъдат използвани за автентикирането на потребитили в VPN и да контролират достъпа до мрежовите ресурси.Недосегаемоста на общата информация през VPN се осигурява чрез методите на криптиране.

В миналото локалните мрежи са били правени чрез наети hard-wired връзки между отделните страни.Тези връзки са били предавани през трафика от един общ клиент.При наследяването на тази концепция върху Интернет, където трафика от много потребители обикновенно минава през същата връзка са били предложени множество протоколи за създаването на

тунелиTunneling –а позволява на изпращачите да капсулират тяхната информация в IP пакети, като тези капсулирани пакети могат да бъдат защитени от подслушване от външни лица използващи техника за криптиране.

Думата “virtual” в VPN означава че мрежата е динамична, с връзки настроени според организационните нужди.Също означава че мрежата е формирана логически въпреки физическата структура на основната мрежа (Интернет в този случай).За разлика от наетите линии в традиционните общи мрежи , VPN не поддържа общи връзки между крайните точки които сформират корпоративната мрежа.Вместо това – връзка се създава само когато има нужда от нея; когато няма нужда от връзка – тя просто се разпада и по този начин мрежовите ресурси са достъпни за другите потребители.По този начин връзките на една VPN нямат същите физически характеристики като hard-wired връзките например.

Тунелите съдържат 2 вида крайни точки – индивидуален компютър или LAN със security gateway, който може да бъде router или firewall.Обикновенно при конструирането на VPN се реализират 2 комбинации на тези крайни точки .

Първият случай: LAN-to-LAN tunneling.Това е сигурен gateway чиито краища служат за

интерфейс между тунела и private LAN-а . В този случай потребителите на друга LAN могат да използват тунела за явна комуникация помежду си.

Втория случай - client-to-LAN tunnels е обикновенно за мобилни потребители които искат връзка с общата мрежа.Клиента, т.е. мобилният потрбител е инициаторът на създаването на тунел от към неговия край за да стане възможна обмяната на информация с общата мрежа.За да направи това той активира специален клиентски софтуер на неговия компютър за да комуникира с gateway защитаващ отдаличената LAN.

Протоколи:

Има 4 протокола за VPN: point-to-point tunneling protocol (PPTP), layer-2 forwarding (L2F), layer-2 tunneling protocol(L2TP), и IP security protocol (IPSec).

Един от първите протоколи за VPN това е PPTP.Той е често използвано решение за dial-in VPN откакто Microsoft включиха негова поддръжка в RRAS за Windows NT Server 4.0 и предложиха PPTP client за service pack за Windows 95.Включването на PPTP client в Widows 98 практически осигури неговото използване за следващите няколко години, въкреки че не е много вероятно PPTP да стане стандарт.

PPTP доизгражда функционалноста на PPP – най често използваният протокол за отдаличен достъп.Той капсулира PPP пакетите използвайки модифицирана версия на GRE – generic routing encapsulation protocol, което дава на PPTP гъвкавостта на handling протоколи различни от IP като internet packet exchange IPE и network basic input/output system extended user interface NetBEUI

Поради зависимоста си от PPP, PPTP разчита на автентикационните механизми в PPP – password authentication protocol PAP и CHAP. Поради силната връзка между PPTP и Windows NT една верия на CHAP, MS-CHAP , също се използва. Той си служи с информация от NT домейни за сигурност.Подобно на това PPTP може да използва PPP за криптиране на информация , но Microsoft са включили силен криптиращ метод наречен Microsoft point-to-point encryption MPPE за използване с PPTP.

Едно от големите предимства на PPTP е че той върви наopen systems interconnection (OSI) layer 2, илиlink layer, за разлика от IPSec, който върви на Layer 3.Тъй като поддържа data communication на Layer 2 PPTP може да предава различни от IP протоколи през тунелите.Все пак PPTP има и накои ограничения – например не осигурява силно криптиране за защитена информация.

L2F също се появява в ранните години на VPN.Също както PPTP , L2F е бил направен като

протокол за tunneling трафик от потребителите до техните корпоративни ресурс и.Главната разлика между PPTP и L2F е ,че поради независимоста на L2F tunneling - а от IP, той може да работи директно с друга медия като смяна на прозорци или asynchronous transfer mode (ATM). Също както PPTP, L2F използва PPP за автентикация на отдаличени потребители но също включва и поддръжка за terminal access control system (TACACS)+ и RADIUS за автентикация.Друга разлика между двата протокола е че L2F позволява тунелите да поддържат повече от една връзка.L2F дефинира връзки вътре в тунела, позволяващо един тунел да поддържа повече от една връзка.

Имаме 2 нива на автентикация на потребителя – първо настройването на tunnel от ISP представителя и второ при настрйките на общия gateway. Поради факта че L2TP е layer-2 протокол, той предлага на потребителите същата гъвкавост като PPTP за handling протоколи различни от IP – като IPX и NetBEUI.

L2TP е направен от една ITEF работеща група като явен наследник на PPTP и L2F, насочен към слабостите на тези протоколи и с намерението да стане IETF стандарт . L2TP използва PPP за да осигури dial-up access. L2TP обаче използва собствен tunneling протокол, базиран на процеса в L2F.

Тъй като L2TP използва PPP за dial-up връзки, той включва автентикационните механизми в PPP, наречени PAP и CHAP. Подобно на PPTP , L2TP поддържа разтегателен автентикационен протокол за други автентикационни системи, като RADIUS.PPTP, L2F и L2TP не включват процесът на криптиране или процесът за създаване на криптографски ключове изискван за криптиране в техните спецификации.Настоящия L2TP планов стандарт препоръчва използването на IPSec за криптиране и за key management в IP среди.

Последният, но може би най важен протокол – IPSec изниква от усилията да се подсигурят IP ракетите като следващото поколение IP (IPv6). Той може да се използва също с IPv4 протоколиIPSec позволява на изпращача да автентекира или да криптира всеки IP пакет или да кандидатства за двете операции в пакета.Отделяйки приложението от packet автентикацията или криптирането е довело до два различни начини на използване на IPSec, наречени modes.Втранспортния mode, само сигмента на транспортния слой на IP пакета се автентицира иликриптира. Другия подход при който се автентекира или криптира целия IP пакет се нарча tunnel mode.Докато transport-mode IPSec се оказва подходящ в много от случаите, то tunnel mode IPSec предоставя още по-голяма защита срещу определени атаки, и подслушване на трафика през Интернет.IPSec е направен на

базата на множество стандартизирани криптографски технологиии за да осигури конфендициалност, цялостност на информацията и автентикация.

Инсталиране и кофигуриране

Windows (95-OSR2/98/ME/NT/2000/XP)

1. Първо трябва да бъде свален клиентски софтуер
2. Ако се използво Windows XP горещо се препоръчва инсталирането на Service Pack 1 преди инсталирането на VPN client, тъй като има бъг в XP, който може да причини инсталационен проблем
3. Да споменем, че ако на машината има инсталирана предишна версия на клиентския софтуер, то тя трябва да бъде деинсталирана
4. Стартиране на инсталацията. За Windows 2000 или XP потребителят трябва да кликне “Yes” за да деактивира IPSec policy agent.
5. Рестарт и след това стартиране на VPN client – а от Start Menu - то

Ако потребителя иска системата да се автентекира на Windows NT domain или на Windows 2k/XP active directory, трябва да се изпълнят следните процедури:

Windows NT/2k/XP Domain

1. Активиране на "Start VPN before logon" от Options -> Windows Logon Properties и проверка на "Enable start before logon". Забележка:Това ще деактивира Fast User Switching в Windows XP.
2. Добавяне локалния WINS сървър към network interface card configuration.Рестарт
3. Стартиране VPN.
4. Веднъж когато VPN е стартиран , добавяне машината към домейна
5. Logout,Рестарт
6. След рестарта потребителя ще бъде попитан дали да се автентекира. Автентекира се към домейна и има достъп до всички свои MS мрежови ресурси върху VPN tunnel-a.

Windows 2k/XP Active Directory

1.А ктивиране на "Start VPN before logon" от Options -> Windows Logon Properties и проверка на "Enable start before logon". Забележка:Това ще деактивира Fast User Switching в Windows XP.

2.Ако активната директория съществува в UF домейн пространството, това е неговия легитимен DNS domain който е бил

делегиран от главния сървър до Microsoft DNS server running AD, и няма да има нужда от някои специфични клиентски конфигурации.Ако обаче не е това случаят ще трябва да се постави локална ия DNS сървър в network interface конфигурация и да се използва **campus tunnel**. VPN тунела по подразбиране ще пренапише DNS сървърите с campus root сървърите.

4. Logout, рестарт

5.След рестарта ще бъдещопитан дали да се автентекира.Автентекираш се към активната си директория и има достъп до всички свои MS мрежови ресурси върху VPN тунела

- Ако VPN клиента е с проста добавка на firewall, като например Cisco VPN client, не се препоръчва нейното използване ,тъй като може да се намеси в tunneling-а .Ето защо се препоръчва Zone Alarm с VPN клиента тъй като той защитава и двете tunneled и non tunneled връзки на сиситемата.
- Както е случая при Cisco client 3.6.1 или по горна версия, има една нова функция която е неактивна по подразбиране - “Automatic VPN Initiation”.Тази функция автоматично стартира VPN клиента ако потрбителя е на campus

жична или безжична автентикационна мрежа.За да се активира тази опция трябва просто да се отиде на Options ->Automatic VPN.

- VPN клиента може да има няколко входа за връзка.Това е полезно ако трябва да се поддържат отделни usernames за тунели на един и същ клиентски софтуер.Препоръчва се да се открие нов вход за връзка чрез “клониране”на UFL VPN връзка Ако откривате абсолютно нов connection entry , той няма да има точните идентифициращи параметри Може да се клонира UFL VPN чрез избирането му в “Connection Entry” dialog box на главният VPN клиентски прозорец и кликване върху Options->Clone Entry.Ще бъдем попитани за име на новата връзка.

Linux kernel 2.2/2.4

1. Първо трябва да бъде свален клиентски софтуер
2. Ако на машината има по-стара версия на клиентски софтуер - то рябва да бъде деинсталиран
3. Ще ни трябва директория vpnclient. След това – vpn_install

4. Ще бъдат зададени няколко въпроса които специфицират инсталацията и предпочитанията.Трябава да се избере ‟yes ” за “start the vpn service at boot time”
5. Рестарт. Това ще осигури правилното въвеждане на VPN модула.
6. Ако се използва ipchains или ipfilter(по подразбиране в Redhat 7.2 и нагоре) или друг тип firewall на linux платформата ще трябва да се разработи за VPN връзка.Ако се използва явен tunneling, който е по подразбиране за UF клиента , ще се наложи да се отворят следващите портове – 128.227.166.116 – 118
    - TCP port 32611
    - UDP port 500

    Ако явния tunneling е деактивиран : 128.227.166.116-118

    - IP protocol 50 (ESP)
    - UDP port 500

Linux kernel 2.2/2.4 Operation

Starting a VPN session:

1. За стартирането на VPN сесия се пише командата - **vpnclient connect ufl-vpn**
2. Въвежда се username във формата "username@ufl.edu" То ще бъде запомнено за по нататъшни VPN действия.Потребителя ще

бъдеш попитан и за парола – това ще бъде “gatorlink” паролата .

3. Ако автентикацията е успешна ще получава съобщение за IP адреса на endpoint-а на тунела. Няма връщане в промпта. VPN client командата ще стои на преден план.Много е важно да не се преписва vpnclient командата , тъй като това ще прекъсне тунела.Ако потребителят иска да премести vpnclient командата на заден план – ctrl-z и после написва bg
4. Ако потребителят иска статистика на тунела – **vpnclient stat**
5. За да бъде прекратена една сесия- **vpnclient disconnect** и ще се появи съобщение съобщаващо че процесът е преустановен

Palm/PocketPC

Ето и някои инструкции за конфигуриране и инсталиране на VPN client за Palm or PocketPC платформи.Ще използваме third party Movian VPN client от Certicom

1. Download и Install Movian VPN client-а
2. Потребителя трябва да рестартира Palm или PocketPC устройството. Това ще осигури правилното инсталирне на IPSec driver
3. Активиране на Movian VPN client

4. Някои оформления които трябва да се наравят в “Policy” прозореца:
    - Policy името трябва да е нещо изразително като “UFL VPN”
    - От pull down листата трябва да бъде избрано "Cisco VPN Concentrator 3000"
    - Gateway адреса е 128.227.166.116
5. Някои оформления които трябва да се наравят в group и user configuration прозореца:
    - Group Name: **vpn-auth-ext**
    - Group Password: (Изисква се gatorlink автентикация).
    - Username: Това е gatorlink username във вида **username@ufl.edu**
6. Натискане на "IKE Suite" бутон
7. В IKE Suite window :
    - Group: **GRP2_DH-1024**
    - Cipher: **3DES_CBC**
    - Hash: **SHA**
8. Натисни "Continue",след това "IPSec Suite"
9. Смяна на Suite с **ESPIP_3DES_SHA-96**.
10. Натискане на "Continue", и после "Done".

Palm/PocketPC Operation

Стартиране на една VPN сесия:

1. След като вече е стартирал Movian VPN client, потребителят трябва да избере Policy, дефинирана отгоре.”Login”

2. Ще се появи промпт за въвеждане на парола. Трябва да бъде въведена gatorlink паролата
3. Натисни “OK” после “Exit”. Тази команда ще затвори само login прозореца.

1. За да видиш и кой е VPN IP адреса потребителя ще трябва да кликне на "Tools->View IPsec Policy"
2. За приключване на сесият – logout

Denial of Service атаки:

Много често еднаDoS атака предшества истинската атака.Ето защо трябва да се обърне много сериозно внимание на това.В безжичния свят на VPN тази атака може да се появи от всякъде и най-основните видове на DoS атаки могатда бъдат толкова обезпокояващи колкото и другите по важни атаки.Тъй като много безжични мрежи използват чистота която се използва масово даже и в някои уреди като микровълнови печки и безжични телефони то хакерите имата възможност за лесно осъществима DoS атака.Пускане на някакъв шум на тази чистота може да причини спиране на работата на мрежата.

По усъвършенствана атака може да се постигне ако хакерът изпрати голямо количество с “разделени” команди като по този начин изкарва

всички потребители в района на атаката извън строй. Друга вариация е когато хакерът разпраща периодично такива команди които не позволяват на нормалният потребител да възстанови връзката след като тя е е прекъсната веднъж .Като добавка към тези атаки хакерите използват злоупотреба на Extensible AuthenticationProtocol (EAP) за осъществяването на DoS атаки. Те могат да манипулират EAP протоколи чрез прицелване в безжични станции и точки на достъп с log-off команди, старт команди , преждевременни съобщения за свързване, failure съобщения , и други модификации на EAP протокола.
По новите DoS атаки използват неправилно конфигурирани безжични мрежи или измамни точки на достъп за да се прицелят в цялата мрежа на някоя организация например.Когато един access point е прикрепен към нефилтриран сегмент на мрежата той разпраща “Spanning Tree” Пакети. Това отваря процеп за атаки вътре в мрежата.
Spanning Tree алгоритъма осигурява съществуването на loop-free Ethernet топология в мрежи които съдържа паралелни мостове и множество Ethernet сигменти.Loop се появява когато има сменящи се маршрути между хостовете.Ако loop съществува в една разширена мрежа , мостове могат да подпомогнат на трафика да объркат Ethernet хостовете, което може да доведе до увеличаване на трафика и разбиване на мрежата до такова ниво ,че скоро няма да може

да работи.Хакер може да усъществи DoS атака чрез умишлено вкарване на този loop в мрежата.Той минава през безжичната мрежа за да отговори злонамерено на променяща се Spanning Tree сесия вътре в предприятието.
Един измамен Kismet sniffer може да усъществи тази атака чрез извикване на повторение на Spanning Tree сесия вътре в мрежата, което връща извиквания на такива пакети със силата на домино.Spanning Tree атаките блокират интелигентните хъбове, мостове рутери и суичове и обикновенно е нужно рестарт за тяхното опряване.
Едно решение на посочения проблем това е AirDefense. Той осигурява постоянно следене на състоянието на радиовълните през цялото време и много лесно може да се распознае атакуващата среда и да се вземат адекватни мерки.

Друга DoS атака това е Ping of Death.Тя е един голям ICMP пакет.Целта приема пинга на фрагменти и започва да ги събира.Тъй като размера на пакета е прекалено голям веднъж събрал се отново той препълва буфераТова предизвиква непредвидими резултати, като рестартиране или забиване на системата. Windows NT е податлив на изпращането на такива пакети. Чрез простото набиране “ping -165527 –s target” може да бъде изпратен такъв ping.Съществува и сорс код за пращане на такива

пакети и на Unix платформи. Такъв код може да бъде намерен много лесно тъй като се разпространява свободно.За да се предпази потребителя от Ping of Death той трябва да има patch да има Firewall

Друга DoS атака това е SYN Flood attack.В TCP IP за да се осъществи комуникация е необходима процедура на три стъпки 3 (3-way handshake).Изпраща се SYN пакет от потребител до услугата, на който се отговаря с SYNACK. На последната стъпка потрбителят отговаря на SYNACK и връзката се осъществява.SYN Flood атака е когато клиента не отговаря на SYNACK и продължава да изпраща SYN пакети.Атакуващия изпраща голям брой фалшифицирани SYN пакети от името на различни недостъпни машини.Операционната система на жертвата им отговаря по нормалния начин като ги добавя в опашката заTCP връзки в състояние SYN_RCVD т.е. чакащи да завършат своя 3-way handshake.Тъй като няма кой да завърши handshake-а опашката се препълва с чакащи връзки.Операционната система започва да не приема нови заявки за TCP връзки на атакувания порт.
Начини за защита – не се използва опашка за частично отворените TCP връзки, информацията за опашката се кодира в ISN чрез криптографски алгоритми.В Windows няма защита.

Пробиви в сигурността.

VPN client software не контролира какъв трафик минава през вътрешната мрежа.Дори в повечето конфигурации това не се прави и от VPN endpoint-а , който може да е firewall, специално VPN приложение или софтуерно базиран VPN сървър.VPN endpointa може да се намира в firewall-а , след firewall-а(Cisco), вътре в вътрешната мрежа или пред firewall-а. Освен в последната конфигурация нападателя може да проникне в системата почти безпроблемно. Обикновенно адреса на атакуващия се появява като част от вътрешната мрежа, зависейки как е конфигуриран VPN клиента.

Клиентския VPN софтуер е силно дружелюбен с атаки от типа на Троянския кон като SubSeven, която предоставя възможност за отдаличено сканиране и пренасочване на връзките.Атакуващия може да конфигурира Троянския кон така че да пренасочи трафика през отдаличена система във вътрешнат мрежа.Пренасочения трафик има същия сорс адрес като отдаличената система и използва същия VPN тунел.За атакуващия- живота е прекрасен, за защитаващия - VPN и firewall не работят както се очаква.

Ето и някои от често срещаните уязвимости при клиентския софтуер на Cisco

В една от уязвимостите наречена от Cisco CSCea77143, атакуващия може да влезе в системата на една частна мрежа от точка в публичната мрежа, без никаква форма на автентикация.Това може да се случи ако IPSec върху TCP е активиран на порт на VPN concentrator. Атакуващия има достъп до всеки хост през този порт.

Друга уязвимост на VPN - CSCdz15393 може да доведе до DoS атака върху VPN concentrator-а.Деформиран SSH инициализиращ пакет изпратен през intitial SSH setup-а може да накара concentrator-а да рестартира.

Друга трета уязвимост - CSCdt84906, наводняване с деформирани ICMP пакети може да дооведе до разбиване работата на концентратора или до рестарт.

Ъпгрейд с последните версии на техния клиентски софтуер Cisco VPN 3000 series concentrators и Cisco VPN Hardware Client , версия 4.0.1 и 3.6.7F, ще успее да защити потребителя срещу тези дупки в сигурноста

Друг вид атаки са така наречените “Man in the middle” атаки.Една такава атака може да разбие връзката между авторизиран station и access point.Успявайки да проникне по средата между

тези 2 структури хакера се превръща в Man in the middle, измамвайки потребителя че той е access point – а,и измамвайки а ccess point-а че той е авторизираната страна.В началото на атаката хакерът следи station- а по време на свързването му с access point –а и по този начин събира автентикационна информация, като име на потрбителя, име на сървъра, клиентски и сървърски IP адрес и др.Хакера след това се опитва да осъществи връзка с access point-а представяики се за автентикационната станция.Access point-а отговаря изпращайки VPN изискването на authenticated station- а, който изчислява изискания автентекиращ отговор и го изпраща на access point-а.Хакера улавя валидния отговор.След това той може да се представя свободно за access point-а.Station-а пресмята правилният отговор който е изпратен до access point-а. Access point-а изпраща след това пакет с прикрепени поредни номера.И двете са изчислени от хакера.Хакера вече е събрал нужната информация за да довърши атаката си и да разбие VPN.

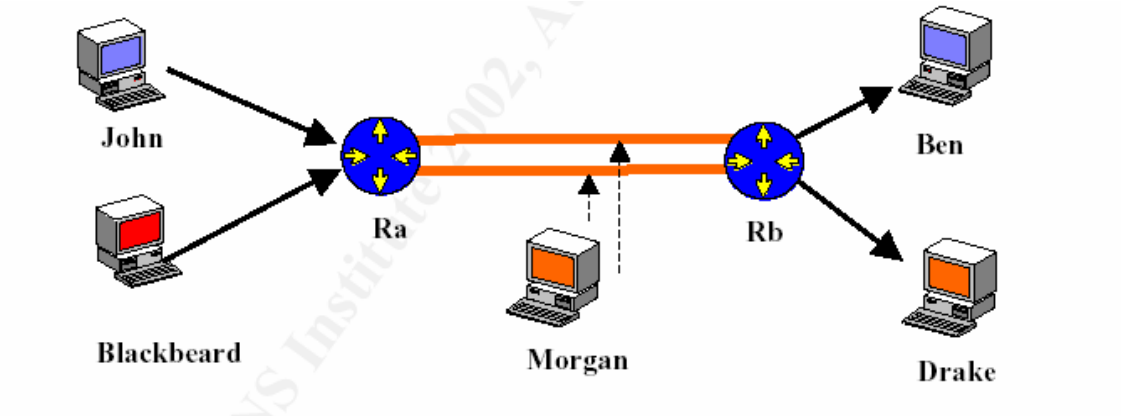
Хакера изпраща лъжлив отговор с големи поредни номера, които разбиват station-а на жертвата.Тогава хакерът прониква в мрежата като авторизирана станция.

Само постоянно наблюдение на трафика и високо надежден IDS може да засече този тип

атака.Ефективно решение на сигурността постоянното наблюдение върху мрежата и анализа на нейната активност. IDS може да засече този вид атаки базиран на сигнатура като едновременно използване на единичен MAC адрес и потребителско име както от авторизираната станция така и от хакера.

Ето и демонстрация на 2 атаки представени от Веселин Цветков от Bohum University , Германия.
Cut-And-Past Attack:
Атаката е възможна само върху две мрежи които използватIPSEC като тунел между двата рутера които свързват мрежите.Има също изискване нападателя да има достъп до втора машина във всяка от двете мрежи.
Morgan sniff-ва легитимен криптиран пакет от John до Ben.Morganсъщо sniff-ва пакет пратен от Blackbeard до Drake.Рутер B е измамен чрез дешифриране на пакета на John за Ben и изпращането му до Drake.Този експлойт не е толкова явен както може да се появи , тъй като има някои изисквания отнасящи се до поредните номера използвани в IPSEC пакетите и осигуряващи ,че оригиналните пакети на John, не достигат рутер B преди фалшивите пакети да го направят. IPSEC включва различни методи за защита от replay атаки, което ще направи тази

атака малко трудна за реализация в истинския свят.



Session Hijacking:
Подобно на предишната атака, Blackbeard има достъп до пакети които е трябвало да пристигнат до Ben ,изпратени от John.Вместо да краде пакетите на John и да пита рутер B за тяхното дешифриране за Drake, Morgan сега поставя информацията на Blackbeards в на John пакета и тя е дешифрирана от рутер B и изпратена на Ben като че ли идва от John.На практика тези атаки са много по сложни за извършване, тъй като поредните номера и някои други автентикационни методи трябва да бъдат преодоляни.