Софийски университет "Св. Климент Охридски"
Факултет по математика и информатика

ДИПЛОМНА РАБОТА

НА

Ирена Иванова Николова

Фак. № М21870

Специалност: Разпределени системи и мобилни технологии

Образователно-квалификационна степен: Магистър

Тема: ***Методи и средства за защита при мрежови комуникации***
(Одит на сигурността в университетската мрежа на СУ)

Ръководител:
д-р Стефан Димитров

София, 2007г.

Съдържание

Увод

„Сигурността е предимно суеверие. Тя не съществува в природата, и хората не могат да я изпитат. Избягването на опасността е това, към което се целим.”
Хелън Келър, Отворената врата (1957)

В съвременния цифров свят, нуждата от мрежова сигурност е повече от очевидна. Компаниите и организациите, притиснати от днешният забързан живот, са задължени да осигуряват множество услуги през Интернет и все по-трудно успяват да предпазят своята поверителна информация от външни лица. Всяка успешно проведена атака може да навреди много, затова инвестициите в мрежова сигурност растат всяка година.

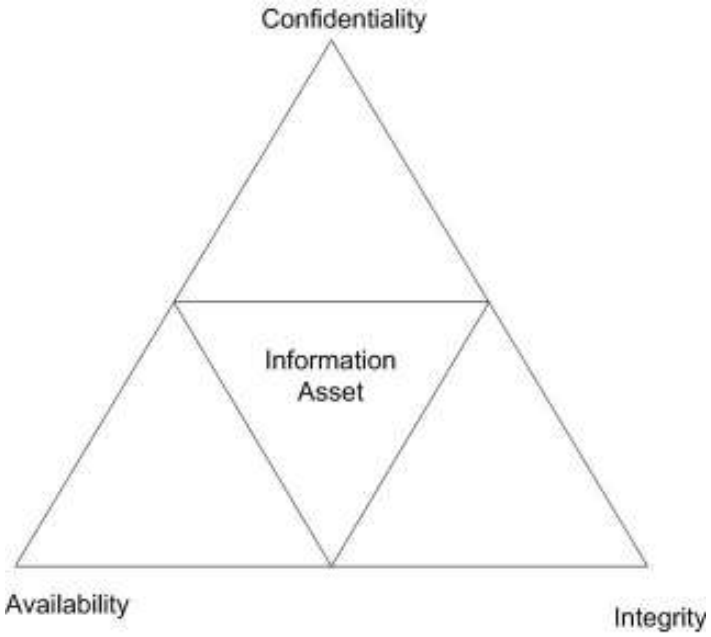
Глава I. Мрежова сигурност – дефиниция и критерии за сигурност

1.1 Предизвикателствата за сигурността

Осигуряването на добра вътрешно-мрежова сигурност и поддържането на възможно най-новите хардуерни и софтуерни продукти е неспиращ процес.Всеки специалист по сигурността се стреми да постигне възможно най-високото ниво на сигурност, тъй като рисковете са реални, а залогът е голям. Организацията трябва сама да реши какво ниво на сигурност й е необходимо, като се вземат предвид както нещата, които трябва да се защитават, така и нужните за това средства, персонал и обучение. Перфектна 100% сигурност не съществува, трябва обаче да се стремим тя да е възможно най-добрата, създавайки си план за управление на познатите рискове и за предпазните мерки за потенциалните такива.
Дефинирането на политика за сигурност в една организация е първата стъпка при осъществяването на сигурността.
Съществуват много средства за IT сигурност, които помагат да се намали уязвимостта на мрежата. Например една защитна стена (firewall) може да бъде реализирана в мрежата, за да предотврати множество атаки. Но тя е само една малка част от инфраструктурата на мрежовата сигурност.
Добра сигурност при крайните устройства, регулярни оценки на общото ниво на уязвимост на мрежата (одити), добри практики за аутентикация, оторизация и отчетност, системи за засичане на проникванията в мрежата – всички те са се превърнали в почти задължителни средства при борбата с мрежовите атаки и осигуряват на специалиста по сигурността по-спокоен сън.

1.2 Дефиниране на критерии за сигурност

Целта на информационната и мрежова сигурност е да осигури надеждност, цялостност и поверителност на информацията (availability, integrity, and confidentiality)(**Фиг.1.1**).
Значението на тези три термина е описано по-долу.
Различните системи и бизнес процеси отдават различно влияние на всеки от тези три характеристики.Така например, въпреки че доставчиците на Интернет услуги (ISP) ще се интересуват от поверителността на данните и тяхната цялостност, по-важно за тях ще бъде да осигурят „висока надеждност” на своите клиенти. Военните ще наблягат на поверителността на данните, като се има предвид техните системи за класифициране на информацията и специалните разрешителни за достъп на хората до нея. Една финансова институция ще се стреми и към трите елемента на сигурността, но най-много ще се стреми на цялостност на информацията.



Фиг 1.1 Балансът между надеждност,цялостност и поверителност на информацията.

За сигурността трябва да се мисли още докато се прави логическият дизайн на мрежата, защото въпросите, които сигурността повдига, могат да повлияят на същинската, физическа топология на мрежата. Трябва да са известни всички спецификации за вида на мрежовите устройства, версиите и възможностите на софтуера и също така да се осигурят специални устройства, осигуряващи криптиране, качество на услугата (quality of service) или контрол на достъпа (access control).
Добра практика е мрежите да бъдат сегментирани, за да осигурят разпределение на отговорността. Отделите като например Финанси, Експлоатация и Поддръжка или Бизнес Развитие могат да бъдат отделени така, че само хора, които имат нужда да достъпват определени ресурси от тези мрежи, да могат да го правят. Нужно е да се определят ресурсите, които ще се защитават, заплахите за тях и границите, в които трябва да се простира политиката на сигурност, която прилагаме. Нужно е също така да се определи нивото на надеждност, поверителност и цялостност, необходими за контролирането на достъпа до тези сегменти. Контрола на достъпа до мрежата със защитни стени, маршрутизатори, комутатори и сървъри за отдалечен достъп и за аутентикация, може да намали значително трафика до критичните устройства и да го ограничи да бъде само от оторизирани потребители или услуги.
Нужно е също така всички сигурни конфигурации да се обновяват своевременно като винаги сме сигурни, че те отговарят на политиките за сигурност, които са наложени. По време на експлоатацията на една мрежа се правят много промени, които често отварят нови уязвимости и дупки в сигурността. Нужно е непрекъснато да се прави оценка на текущото ниво на мрежовата сигурност и своевременно да се взимат мерки за всяка нов открит евентуален проблем.

1.2.1 Надеждност

Това наричаме свойството информацията и услугите да са достъпни и работещи винаги, когато е нужно. Резервираност, устойчивост на сривове, достъпност, автоматично заработване на резервният модул, в случай че активният отпадне

(failover) , архивиране и възстановяване на данни (backup and recovery), гъвкавост, разпределяне на натоварването (load balancing) – това са основните концепции на мрежовият дизайн, който би ни осигурил висока надеждност. Така например, ако системите са недостъпни, тяхната цялостност и конфиденциалност е вече без значение за крайният потребител или клиент.
Сиско Системс (Cisco Systems) произвежда и поддържа много системи, проектирани за висока надеждност.Тези системи имат много дълго време между техническите повреди (mean time between failure – MTBF). Те обикновено са с резервирани захранвания за ток, с карти (чипове) и модули, които могат да се сменят в реално време (hot-swappable). Такива устройства могат да осигурят 99,999% процента надеждност, което означава по-малко от 5 минути на година през които системата не функционира (downtime).
Надеждността на отделните устройства може да бъде повишена при конфигурирането им. Използването на резервирани линкове със HSRP (Hot Standby Redundancy Protocol), на Spanning Tree Protocol за бързо адаптиране на мрежата след неочаквано отпадане на устройство или линк (fast convergence) или групирането на няколко физически линка в един логически (EtherChanel), всичко това са техники, благодарение на които мрежата може да продължи да функционира правилно, дори и при отпадането на даден неин компонент.

1.2.2 Цялостност

Целостта е свойството на информацията или дадено приложение да са завършени, прецизни и проверени. Искаме да предотвратим неоторизирани хора или процеси да правят промени по системата, така както и оторизирани хора да правят неоторизирани промени по нея – без значение дали тези промени са неволни или умишлени.
В контекста на мрежите това означава да се убедим, че съобщението, което е получено, е същото като това, което е изпратено. Съдържанието на съобщението трябва да е цяло и непроменяно, докато се предава между истинският подател и получател. Това може да се постигне с криптиране и контрол на маршрутизирането. Целостта също може да се отнася и за операционните системи на мрежовите устройства, които пренасят данните. Трябва да сме сигурни, че не са преднамерено променяни или пък повредени.

1.2.3 Поверителност

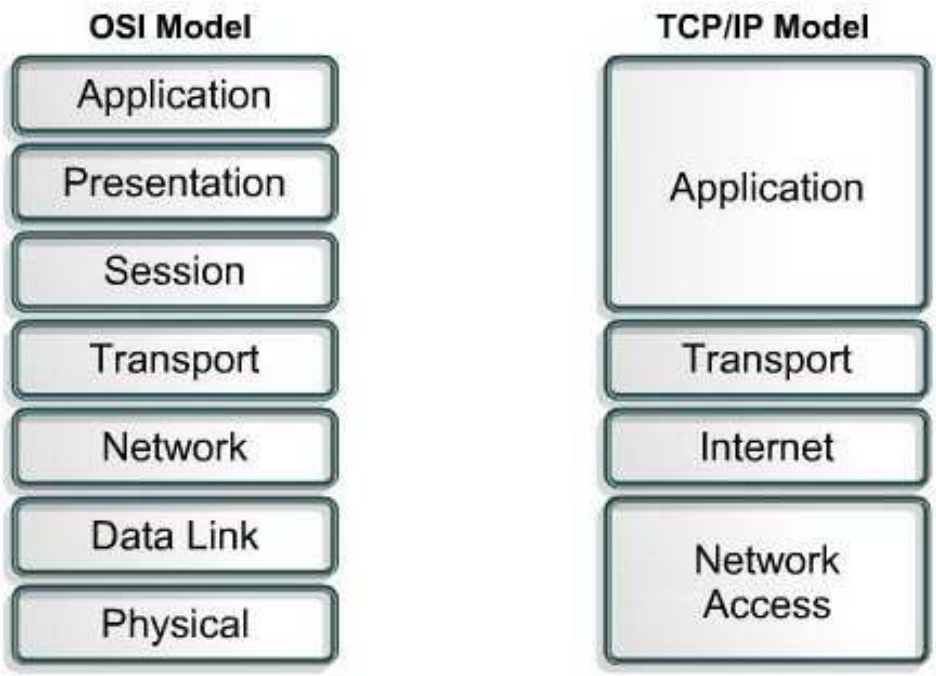
Поверителността защитава важната информация от неоторизирано откриване или подслушване. За това се използват криптографията и контрол на достъпа. Усилията, положени за запазване целостта на информацията, зависят от важността и и от това до колко е допустимо тя да бъде наблюдавана или подслушвана.
Криптиране в мрежите може да се приложи на всеки слой от протоколния стек. Приложенията могат да осигурят криптиране от подателя до получателя, виртуални частни мрежи(VPN), могат да се използват за изграждане на сигурен канал на мрежовият слой. Криптиране може да се използва и в каналния слой от OSI модела (data link layer), но на този слой то може да бъде само от точка до точка и не е много полезно, защото по този начин всяко едно устройство, което приема и предава пакета, трябва да участва в това криптиране/декриптиране. На най-долният слой се следи за физическата сигурност – не се разрешава неоторизиран достъп до мрежови портове или устройства. Големият проблем на по-долните слоеве е закачането на системи за следене на трафика (sniffers) или анализатори на пакети към мрежата.

1.3 Въведение в мрежовата сигурност

1.3.1 Мрежови комуникации в TCP/IP

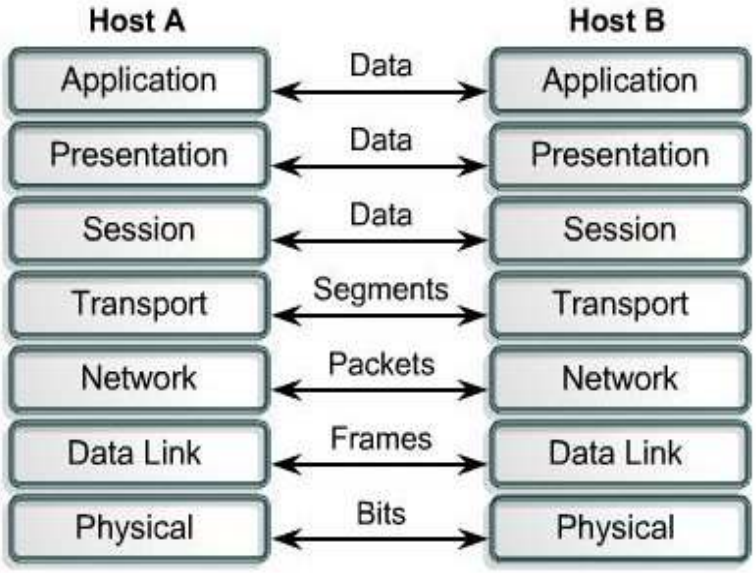
Протоколният стек Transmission Control Protocol/Internet Protocol (наричан накратко TCP/IP) на практика вече се е превърнал в стандарт за комуникация в компютърните мрежи заради своята гъвкавост и удобство.
Този стек представлява съвкупност от известен брой протоколи и приложения, които работят на различни логически слоеве. Всеки слой отговаря за различен аспект на комуникацията.
TCP/IP Internet моделът е съставен от 4 слоя (**Фиг. 1.2**). TCP/IP слоевете са сравнени със съответните им 7 слоя при OSI (Open Systems Interconnection) модела.

Фигура 1.2 Слоевете от TCP/IP протоколният стек,сравнени със слоевете на OSI модела .



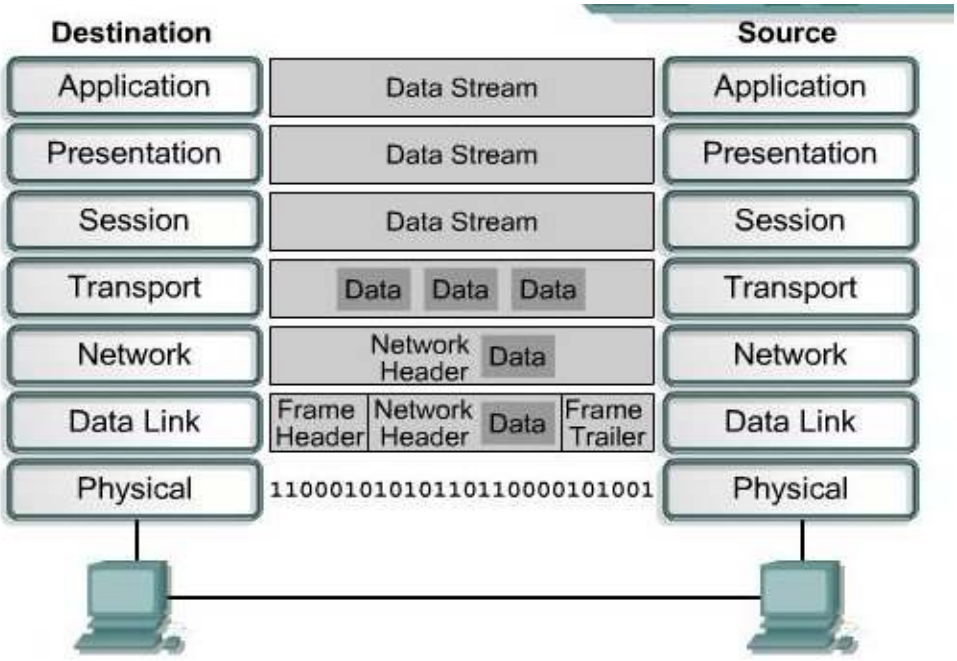
Разделените на слоеве протоколи са замислени така, че всеки слой при получателя приема данните, изпратени от същият този слой и при изпращача. Всеки слой си комуникира само със съответният от отдалеченият хост, не се интересува от параметрите или формата използвани в слоевете под и над него.(**Фиг 1.3**)

Фиг 1.3 Логическа и физическа комуникация между протоколните слоеве.



При предаване данните преминават по посока от горе надоле: от приложния към транспортния, мрежовия и каналния (data link) слой и всеки протокол слага своя заглавна част (header) и “опашка” (trailer) на пакета, капсулирайки по този начин потребителските данни, заглавията и опашките на по-горните протоколи. При системата, която получава информацията, тези хедъри се премахват при преминаването на данните от по-долен слой към по-горен. Този метод е много гъвкав, защото по-горните слоеве нямат нужда да знаят каква технология се използва отдолу. **Фиг 1.4** показва пример за това как се извършва капсулацията при изпращача.

Фиг. 1.4 Капсулиране при протоколните слоеве.



Кратко описание на слоевете в TCP/IP модела:

-*Приложен слой:*
Той осигурява трансфер на файлове, бази данни и съобщения, принтерни и терминални услуги. Някои от протоколите, които работят на този слой са: HyperText Transfer Protocol (HTTP), Telnet, File Transfer Protocol (FTP) и Simple Mail Transfer Protocol (SMTP).

-*Транспортен слой:*
Осигурява комуникация от една крайна точка до друга крайна точка (end-to-end) между процеси, изпълнявани на различни хостове. Предоставя на по-горните слоеве услуги със или без установяване на свързаност (connection-oriented или connectionless), в зависимост от застъпените протоколи. Слоят използва номера на клиентски и сървърски портове, за да индетифицира различните процеси, изпълнявани на този хост. Там се сегментират данните, подадени му от сесийният слой, назначавайки пореден номер на всеки сегмент, с цел правилното им подреждане от получателя. Слоят организира потока от данни и осигурява контрол при положение, че сесията е с установяване на свързаност. Протоколи, отнасящи се към транспортният слой, са TCP и UDP (първият осигуряващ надеждност, а вторият бързина при трансфера на данните).

- *Интернет (мрежов) слой:*
Една от основните му функции е задаването на логически адреси на източник и местоназначение, както и определяне на най-добрият път за маршрутизиране на данните между мрежите. Също така е отговорен и за откриването и уведомяване за грешки, разделянето и събиране на пакетите на рамки - фреймове. Последното се случва точно в този слой, защото различните мрежови технологии имат различни изисквания за максимална дължина на пакетите - Maximum Transmission Unit - MTU). Протоколите, които се използват в този слой, са Internet Protocol (IP), Internet Control Message Protocol (ICMP) и Address Resolution Protocol (ARP).

- *Слой на мрежовия достъп:*
В този слой можем да включим мрежовите карти и драйверите на устройствата. Те представляват физическия интерфейс към мрежовата среда. Този слой контролира хардуера, капсулира в рамки (фреймове) и изпраща идващите от по-горния IP слой пакети, приема и разкодира пристигащите.

1.3.2 Сигурност в TCP/IP стека

Интернет мрежата не дава никаква гаранция за поверителност на информацията. Затова винаги, когато става дума за важни, ценни или лесно уязвими данни, трябва да имаме предвид криптографията - т.е информацията да се криптира преди да се изпрати и да се декриптира, чак когато пристигне при получателя. Повечето слоеве в OSI модела могат да бъдат използвани за осигуряване на цялостност и конфиденциалност на данните. Но прилагането на правила за сигурност на различните слоеве може да има различни предимства и недостатъци.

1.3.2.1 Криптография

Криптографията е наука за създаването и разчитането на кодове или шифри. Информационната сигурност използва криптографски системи, за да пази данните скрити и да разпознава идентичността на изпращача и получателя на данните. Криптографията също така може да осигури цялостност на информацията, тъй като тя позволява само оторизирани хора или процеси да я достъпват и може да открие подправяне или промяна на оригиналното съобщение или файл. Криптографията, казано просто, работи по следният начин: прави усилията нужни да се разбият криптираните данни много по-скъпи отколкото самите данни или съответно разбиването отнема повече време отколкото данните ще продължават да бъдат ценни.
Има три вида криптографски функции: със симетричен ключ, с несиметричен ключ и хеш функции.
Повечето от стандартните алгоритми са отворени и известни на обществото и са били тествани обстойно от много експерти. Тяхната сигурност зависи от силата на алгоритъма и дължината на ключа. Ключът е последователност от битове, която се използва за математическото изчисление на криптиращата и декриптираща информация. Хеш функциите не използват ключ. Хешът се изчислява от специална математическа функция. Съществуват много алгоритми за криптиране на информацията. За да си разменят криптирани съобщения изпращачът и получателят трябва да използват един и същ алгоритъм за криптиране и разбира се един и същ ключ.

1.3.2.2 Криптография със симетрични ключове

Криптографията със симетрични ключове използва един и същ ключ за да криптира и декриптира съобщението. Всяка двойка изпращач и получател използват един и същ ключ, за да си разменят съобщения. Успявайки да криптира и декриптира полученото съобщение, всяка от страните приема, че отсрещната страна е тази, с която е разменил ключове по-рано. По този начин се осигурява някакво ниво на аутентикация. За да работи тази схема е нужно ключовете да се пазят в тайна и да се знаят единствено от двете страни.
Примери за алгоритми, които използват симетрични ключове са:

- Data Encryption Standard (DES) (56 бита)
- Triple DES (3DES) (168 бита)
- International Data Encryption Algorithm (IDEA) (128 бита)
- Rivest Cipher 4 (RC4) (използа ключ с променлива дължина)
- Advanced Encryption Standard (AES) (скоро ще замени DES като стандарт)

Когато имаме съхранени криптираните файлове и симетричният ключ се загуби или повреди по някакъв начин, това може да означава и че вече нямаме достъп до файла. Затова е добра практика ключовете да се съхраняват на друго място,за да се предпази организацията от такъв вид загуби. Симетричният ключ и съответно всички негови копия трябва да се пазят също толкова, колкото и данните, които той защитава. Размяната на ключовете също трябва да се извършва по сигурен начин. Ако някой прихване ключа по време на пренасянето му или по някакъв начин го вземе от системата на потребителя, то тогава може да подслушва без проблем и криптираният трафик. Конфиденциалността и цялоста на информацията вече ще е загубена.
Алгоритмите за криптиране със симетричен ключ са доста бързи и за малко време могат да криптират голямо количество информация. Те са толкова по-силни, колкото по-дълъг ключ се използва.

1.3.2.3 Криптография със асиметрични ключове

Криптографията със асиметрични ключове е по-позната като криптография с публичен ключ. При нея се използват двойка ключове, които са математическа функция един на друг, но ако имаме само единият, е много малко вероятно да изчислим другият ключ. Единият ключ се използва за криптиране и подписване, а другият за декриптиране и проверка за грешки. Единият е скрит и се пази в тайна, а другият е публично достъпен.
Това са няколко примера за алгоритми за криптиране с асиметрични ключове:

- Diffie-Hellman
- Rivest, Shamir, Adleman (RSA)
- Digital Signature Algorithm (DSA) / El Gamal
- Elliptic Curve Cryptosystem (ECC)

Алгоритмите за криптиране с асиметрични ключове са еднопосочни функции. Те могат лесно да бъдат изчислени в едната посока, но изключително трудно в обратната, ако нямаме и двата ключа. Но дори и да притежаваме и двата, асиметричните алгоритми са много ресурсоемки.Те са около 100 пъти по бавни от алгоритмите, които работят със симетрични ключове. На практика не се използват за криптиране и декриптиране на голямо количество информация.
Те работят по следният начин. Когато целта е да се запази поверителността на данните, изпращачът криптира съобщението със публичният ключ на получателя. Само частният на ключ на получателя може да декриптира съобщението. Съобщения, предназначени за повече от един получател, трябва да бъдат криптирани по отделно за всеки един от тях. Когато се използва за аутентикация при електронните подписи, съобщението се криптира с частният ключ на изпращача. Само публичният ключ на изпращача може да го декриптира,потвърждавайки по този начин, че то наистина идва от него. Запазването на поверителността на данните е по-честото приложение на криптографията с публични ключове.

1.3.2.4 Хеш функции

Хеш функциите се използват за да превърнат съобщение с различна дължина в код с фиксирана големина, така нареченият хеш или сума на съобщението. Различните алгоритми създават хеш функции с различни дължини. Някои примери за това са:

- Message Digest 5 (MD5) (128 бита)
- Secure Hash Algorithm (SHA) (160 бита)
- Haval (променлива дължина на хеш кода)

Хеш функциите са криптографска контролна сума, която се използва да провери цялостта на съобщенията. Промяна само на един символ в оригиналното съобщение, би променило голям брой от битовете в хеш кода. Хеш функцията е едностранна функция и е математически невъзможно оригиналните данни да се възпроизведат от хеш кода. Изпращачът изчислява хеш кода на оригиналното съобщение и го изпраща заедно с криптираните данни. Получателят декриптира съобщението и също изчислява хеш кода. Ако оригиналният хеш код е същият като току-що изчисленият, тогава получателят е сигурен,че данните са цели и непроменени.

1.3.2.5 Цифрови сертификати

Цифровите сертификати са структури от данни, подписани от т.нар. доверен доставчик на удостоверителни услуги (certificate authority - CA), който пази в своя база данни кой публичен ключ на коя личност или организация принадлежи и още друга допълнителна информация. Те играят главна роля при разпространението на публичните ключове. Доверието в различните организации зависи от доверието, което имаме на доставчика на удостоверителни услуги, където се пазят данните за тях. Цифровите сертификати се използват, за да се докаже аутентикацията, конфиденциалността и цялостността например при web транзакции, размяна на e-mail съобщения и IPSec. Сертификатът е подписан с частния ключ на доставчика на удостоверителни услуги. Публичният ключ на CA се използва, за да се аутентикира сертификата. Системата за електронно удостоверяване (PKI инфраструктура) дава механизъм за генериране на ключове, за управление на сертификати и осигуряване цялостта на ключовете. Сертификатите се издават с дата на изтичане, след която са вече невалидни. Валидността на сертификата може да бъде прекъсната преди изтичането му, например поради промяна в дадена организация или компания. Валидността на сертификатите се сравняват спрямо така наречените „списъци за анулирани сертификати" (certificate revocation lists - CRLs) или чрез механизъм за online проверки, който да удостовери тяхната валидност. CRLs могат да бъдат свалени от доставчика на удостоверителни услуги и да бъдат използвани офлайн, но трябва да се обновяват периодически. Сертификатите са базирани на стандарта X.509 версия 3. Тази версия подобрява използваемостта на сертификатите, като добавя нови стандартни и незадължителни полета към по-ранния формат. Стандартните разширения включват полета като Key Usage, Private Key Usage Period, Certificate Policies и Policy Mappings.

1.3.3 Контрол на достъпа

Контрол на достъпа е процеса на разграничаването на привилегиите при използването на системните ресурси. Съществуват три начина за контрол на достъпа:

Административен контрол – базира се на политики. Политиките за информационна сигурност трябва да излагат целите на организацията по отношение на сигурността, контрола на достъпа до ресурсите, наемането и управлението на персонала.

Физически контрол – включва физическото ограничаване на достъпа до мрежовите устройства, защита на границите на мрежата и осигуряването на стаи и сгради, в които се намират важни устройства.

Логически контрол – хардуерното и софтуерното значение на фразата ограничаване на достъпа и включва списъци за контрол на достъпа,комуникационни протоколи и криптография.

Контролът на достъп включва проверяване на идентичността на акаунта (аутентикация) и след това даване на права за достъп базирани на тази идентичност (оторизация). Достъпът може да бъде предоставен на човек, работна станция, сървър или услуга. Например услугата „наблюдение и контрол на мрежата" (network management) използва по SNMP протокола т.нар. споделена дума (community string), за да реализира контрола на достъп. Една такава споделена дума дава ограничен достъп на управляващият софтуер до мрежовото устройство, докато друга дава пълен достъп както за четене на данни от устройството, така и за писане върху него. Човек може да достъпи същото това устройство като обикновен потребител с ограничени права или като потребител с пълен контрол. Контрол на достъпа до мрежата може да се осъществи на границите и чрез използването на защитна стена или маршрутизатор, на който са дефинирани списъци за контрол на достъпа.

1.3.3.1 Аутентикация

Аутентикацията е проверка на идентичността, която даден потребител, процес или машина твърдят, че имат. Следващите нива при контрола на достъпа зависят от аутентикацията. На базата на нея се извършва оторизацията, т.е дават се права на точно дадената идентичност. Отчетността също няма да работи, без да я има аутентикацията.
Нивото на аутентикация, изисквано за дадена система, зависи от изискванията за сигурност, идващи от самата нея. Например публично достъпните уеб сървъри могат да позволяват анонимен достъп, както и достъп за гости. Финансовите транзакции трябва да изискват много силна аутентикация. Пример за слаба форма на аутентикация е използването на IP адрес за определянето на идентичност. Подмяната или нелегалното използване на IP адреса може лесно да излъже този механизъм. Силната форма на аутентикация изисква поне два фактора за доказване на идентичността:

Какво знае човек: пароли и лични идентификационни номера (PIN кодове) са пример за това какво човек може да знае. Паролите могат да бъдат за еднократно или многократно използване. *S/Key* е пример за система за еднократни пароли (http://en.wikipedia.org/wiki/S/KEY).

Какво притежава човек: Различни хардуерни устройства или софтуерни приложния: Смарт карти, също така и SecureID, CRYPTOCard, и SafeWord.

Кой е човекът: Биометричните характеристики са това, което показва кой точно е човекът, защото разпознаването на идентичността се базира на физическите му характеристики: например сканиране на дланта, геометрия на ръката, сканиране от ириса на окото, модел на ретината, отпечатъци от пръсти, модел на гласа, разпознаване на лице или подпис.

Съществуват много системи за мрежова аутентикация. TACACS+ (Terminal Access Controller Access System), Kerberos и RADIUS (Remote Access Dial In User Service) са протоколи за аутентикация, поддържани от Сиско.Тези системи за аутентикация могат да бъдат конфигурирани да изпозват много от примерите за установяване на идентичността, посочени по-горе.
Въпреки че това е извън обсега на тази глава, Сиско маршрутизаторите могат да се аутентикират един друг с цел да се докаже, че рутинг промените идват от сигурен източник и не са променяни и повредени. Сиско може да използва MD5 хеш функция или друг алгоритъм. Няколко протокола за маршрутизация, които се използват от Сиско устройства, поддържат аутентикация:

- Open Shortest Path First (OSPF)
- Routing Information Protocol version 2 (RIPv2)
- Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)
- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)

1.3.3.2 Оторизация

Оторизацията е привилегията да се разрешава достъпа до услуги или информация само за определени групи или личности. За системи, които трябва да поддържат високо ниво на сигурност, нивото на достъп по принцип трябва да бъде забранено за всички, като изключенията се добавят допълнително. Дори и добавени

допълнително, правилата за достъп трябва да са на принципа на най-малкото, което е нужно на даден човек. За публични системи оторизация може да се даде и на гости или анонимни потребители. Нужно е да се определят изискванията ни за сигурност, за да се определят подходящите граници на оторизация.

1.3.3.3 Отчетност

Отчетността е записването на цялата мрежова дейност и всички опити-успешни и неуспешни за достъп до мрежовите ресурси. Въпреки че тази информация може да се използва за сметки и фактуриране, от гледна точка на сигурността тя е най-важна за засичане, анализиране и реагиране на инциденти със сигурността в мрежата. Системни логове, периодични прегледи и оценки на състоянието на компонентите на мрежата, както и различните софтуери заедно могат да се използват за следене какво се случва когато даден потребител се логне в системата.

1.4 Дефиниране на политика за сигурност

1.4.1 Какво е политика за сигурност и защо ни е нужна?

Решенията по сигурността, които вземаме или съответно не вземаме, определят колко сигурна или несигурна ще е мрежата ни, какви функционалности ще предлага и колко лесно достъпна ще бъде.
Но при всички положения не могат да се вземат правилните решения за сигурността, ако не се определят първо критериите за сигурността, която се стремим да постигнем. Докато не са ясни тези цели, не можем ефективно да използваме нито един инструмент за сигурност, просто защото няма да знаем какви проверки да правим и какви ограничения да приложим.
Така например нашите цели се различават малко от целите на производителите на обурудване. Те се опитват да направят конфигурацията и работата с продуктите им възможно най-лесна, което обикновено води до това конфигурацията по подразбиране да бъде възможно най-отворената, т.е несигурна.
За да се улеснят инсталирането на новите си продукти, производителите прват лесен достъпа и на неоторизирани лица до тези системи.
Когато се определят критериите за сигурността трябва да се вземат предвид основно следните така да се каже „дилеми“: (RFC 2196)

(1) Услугите, които предлагаме срещу мерките по сигурността, които вземаме.
Всяка услуга, която се предлага на потребителите, крие свой собствен риск за сигурността. За някои от услугите рискът е по-голям отколкото ползата от самата услуга – за тях администраторът може да реши по-скоро да спре да се предоставя, отколкото да се опитва да я направи сигурна.

(2) Леснотата на използване срещу сигурността.
Системите, които се използват, най-лесно биха позволили достъп на всеки, не изисквайки никакви пароли, което би означавало никаква сигурност.
Изискването за пароли прави системата малко по-сложна, но пък и по-сигурна.
Изискването за генерирани от различни устройства пароли, които да са валидни само веднъж, я прави още по-трудна за използване, но пък и много по-сигурна.

(3) Цената на сигурността срещу риска от загуба.

Сигурността може да се измерва в различни стойности: парични (т.е разходите за закупуването на хардуер и софтуер като например хардуерни защитни стени или генератори на пароли за еднократно използване), производителност (т.е криптирането и декриптирането изисква време),и други.

Съществуват също така и различни нива на риска: загуба на конфиденциалността (т.е достъп до информацията от неоторизирани личност), загуба на данни (т.е повреда или унищожаване на информацията) и отказ от услуга (а именно запълване на файловата система, използване на изчислителните ресурси и отказ от достъп до мрежата). Всеки вид разход трябва да се прецени спрямо всеки вид загуба на данни. Резултатите, които се стремим да постигнем свързани със сигурността трябва да бъдат заявени на потребителите, администраторите на системата и мениджърите чрез множество правила на сигурност, наречени „политика за сигурност“. Използваме този термин вместо по-тесния „компютърна сигурност“, тъй като визираме всички видове информационни технологии и данните събирани и обработвани при/от тези технологии.

1.4.2 Дефиниция на политика за сигурност.

Политика за сигурност наричаме формално множеството от правила, по които хората, които имат достъп до технологиите и данните на дадена организация трябва да се ръководят.

1.4.3 Целите на една политика за сигурност.

Основната цел на една политика за сигурност е да информира потребителите, служителите и мениджърите за задължителните изисквания за запазването на информационните технолигии и данни. Политиката трябва да определи механизъм, чрез който тези изисквания могат да бъдат спазени. Другата й цел е да се определят насоки за поддържането, конфигурирането и оценката на компютърните системи и мрежите спрямо тази политика.

Така наречената „политика за правилно използване“(Appropriate Use Policy - AUP) също може да бъде част от политиката за сигурност. Тя трябва да определи какво потребителите трябва и не трябва да правят на различните компоненти на системата, вкючително на типа трафик, разрешен в мрежата. AUP трябва да бъде възможно най-прецизна, за да се избегне двусмислие и неразбиране. Например, AUP може да съдържа списък на всички забранени за достъп сайтове. („Политиката за правилно използване“ често се нарича също и „политика за приемливо използване“.)

1.4.4 Кога една политика за сигурност е добра?

Характеристиките на една добра политика за сигурност са:

(1) Тя трябва да бъде приложима чрез процедури за администрация на системата, като съдържа правилата за „правилно използване“ (acceptable use guidelines), или чрез други приемливи методи.

(2) В нея трябва да има описание на различните средства за сигурност, които ще се използват, където е възможно и разрешено.

(3) Тя ясно трябва да дефинира границите на задълженията на потребителите, администраторите и управленският състав.

Компонентите на добрата политика за сигурност са:

(1) Правилата за поръчка и закупуване на компютърни технологии, които определят нужните или предпочитани характеристики на сигурността. В тях трябва да се включват и съществуващите в момента политики за поръчки на оборудване/технологии.

(2) Политика за конфиденциалността, която определя разумни очаквания за конфиденциалност, по отношение на проблеми от рода на: следене на електронната поща, подслушване на трафика или достъп до потребителските файлове.

(3) Политика за достъпа, която определя правата и привилегиите за достъп, които ще запазят информацията от изгубване или разкриване чрез определянето на правила за потребителите, отговорният персонал и управляващите. Тя трябва да определи условия за вътрешната комуникация, за потока от данни, за добавянето на нови устройства към мрежата или прилагането на даден нов софтуер към съществуващите системи. Тя също трябва да определя необходимите информационни съобщения. Например съобщенията, които предупреждават за нужда от ауторизация и наблюдение на връзката, а не обикновеното и по подразбиране съобщение „Добре дошли“.

(4) Политика за отчетите и отчетността, която дефинира отговорностите на потребителите, отговорният персонал и управленският екип. Тя трябва да определя начините за оценяване и правилата за справяне с инциденти. Т.е, какво да се направи и кого да уведомим, ако открием евентуално нарушение или проблеми свързани със сигурността.

(5) Политика за аутентикацията, която дефинира достоверността в мрежата - чрез ефективна политика за паролите, чрез определяне на правила за аутентикация при логване от отдалечено място и чрез използването на аутентикиращи устойства (т.е., пароли за еднократно ползване и устройствата, които ги генерират).

(6) Изисквания за правилното функциониране на системите, които дефинират очакванията на потребителите за достъпа до ресурсите и системите. Те трябва да описват резервираността и процеса на възстановяване при евентуални сривове, както и да определят часовете, в които ресурсите ще се използват и периодите, през които ресурсите няма да бъдат в изправност заради планирани действия по тях. Те също трябва да включват контатна информация на хората, които отговарят за системата за отчети и мрежовите проблеми.

(7) Политика за Информационите системи и Оперирането с мрежата, която описва как и вътрешните и външните хора по поддръжката ще достъпват и работят върху технологиите. Една важна тема, която трябва да бъде засегната тук, е дали ще бъде позволена отдалечената поддръжка на системите и как ще се контролира подобен достъп. Също така в тази политика трябва да се дефинира дали ще има изнесени извън компанията поддръжка и експлоатация на системите (outsourcing) и как ще се извършва неговото управление.

(8) Политика за съобщаването на нарушенията, която дефинира кои видове нарушения (например по конфиденциалността, по сигурността, било то вътрешна или външна) трябва да бъдат докладвани и към кого да се адресират тези репорти. Една незаплашваща атмосфера и възможността такива отчети да се правят анонимно биха довели до по-голяма вероятност забелязаните нарушения да се докладват.

(9) Допълнителна информация, която помага на потребителите, отговорният персонал и управленският екип да съобщават за нарушения на политиката за сигурност, да предприемат правилните действия при инцидент по сигурността, както и определя кои данни могат да се считат за конфиденциални или лични. Също така тя трябва да съдържа препратки към процедури по сигурността и други материали по темата, като например други фирмени политики, обществени закони и правилници.

Съществуват някои правни проблеми,които биха имали отношение към една политика за сигурност (например следенето на трафика).Затова създателите на една политика за сигурност трябва да имат предвид и легалната и страна. Добре е да се потърси правна помощ при създаването на политиката, или поне тя да се прегледа от юридически консултант.
След като се създаде такава политика за сигурност, тя ясно трябва да се представи пред потребителите, отговорния персонал и управленския екип. Изискването всеки служител да подпише такава политика ще покаже, че я е прочел, разбрал и е съгласен да се ръководи по нейните правила – това е най-важната част от процеса. Последното, което трябва да се добави, е нуждата от редовен преглед на политиката за сигурност, за да се види дали тя все така успешно отговаря на нашите нужди в смисъла на сигурността.

Глава II. Методи и средства за защита при мрежови комуникации

За да можем правилно да изберем подходящите средства за защита, необходимо е първо да знаем от какво ще се защитаваме, т.е. да имаме възможно най-пълни познания относно най-различните типове мрежови атаки.

2.1 Мрежови базирани атаки

За разлика от предишната глава, в която описвах теоретичната страна на информационната сигурност, в тази глава ще се спра на най-основните атаки в мрежата, ще обясня целта им и как се извършват.
Броят на мрежовите атаки в последните няколко години нарасна значително. Едни от най-разпространените атаки са следните:

- Атаки с цел невъзможност за предоставяне на услуга (DoS)
- Разпределени DoS (DDoS)
- Атаки включващи отвличане на сесия (един пример е атаката човек-по-средата (man-in the middle attack)

Изключително важно е да се разбере, че всеки може да извършва тези атаки на всеки. Следователно належащо е специалиста по мрежовата сигурност да разбира напълно начина на провеждане на атаката, за да може да и се противопостави.

2.1.1 Атака от тип DoS

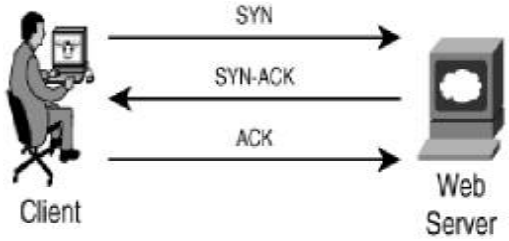
DoS атаките се използват, за да се наруши нормалната операция на дадена система или мрежа. Злодеятелят цели чрез DoS атаката да претовари или спре достъпа до системата или дадения ресурс на мрежа. Такава атака води до 100% натоварване на мрежовите устройства или сървъри и те не могат да обработват подадените им пакети, в следствие на което ги отказват (drop). Целта на атакуващия е да се откаже (спре) достъпа на легитимни потребители до различните услуги. Този вид атаки често се използват наред с други атаки, като целта им е да осакатят системите за сигурност преди реалната атака. Най-често при DoS атака се цели да се наруши мрежовата свързаност, като се опитва да се отворят множество фалшиви TCP или UDP връзки. Устройството, към което е насочена атаката, се опитва да обработи всички заявки за връзки и по този начин се утилизират всички възможни ресурси. Съществуват три DoS атаки, които целят нарушаване на мрежовата свързаност.

- TCP SYN претоварващи атаки
- Land.c атаки
- Smurf атаки

2.1.1.1 TCP SYN претоварващи атаки

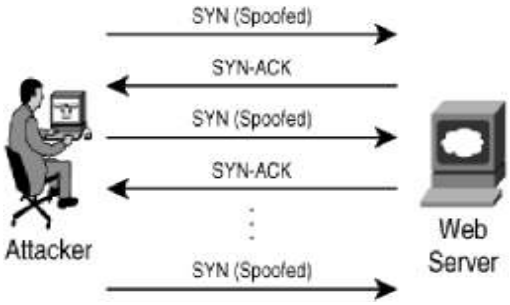
Те са проектирани така че да се възползват от слабостта на TCP протокола и по-специално от процеса на установяване на връзката (TCP tree-way handshake). Установяването на връзката при TCP се извършва от тройна размяна на пакети както е показано на фигура 2.1.

Фиг. 2.1



Клиента се опитва да установи връзка с уеб сървъра. Първо, той изпраща SYN (синхронизиращ) пакет до сървъра с цел да се синхронизират поредните номера на клиента и сървъра. SYN пакетът съдържа ISN (initial sequence numbers) на клиента. SYN, ACK, RST и други са всъщност битове (флагове) от хедъра на пакета. В този първи т.нар. SYN пакет, SYN=1, ACK=0. При вторият пакет подателят вече е сървъра и той едновременно потвърждава че е получил ISN номерата на клиента, и изпраща своите ISN номера (SYN=1, ACK=1). Сървърът увеличава с единица поредния номер на клиента, и го изпраща обратно на клиента като свой acknowledgment номер. Последната стъпка в този процес на обмяна, е пак от страна на инициализатора, който изпраща ACK пакет на сървъра. Връзката вече е установена.

Фиг. 2.2



При TCP SYN претоварването имаме претоварване на мишената на атаката чрез използването на множество подправени SYN пакети, които симулират валидни заявки за връзки. Тези пакети биват изпратени на сървъра все едно са начало на уговарянето на конекция, сървърът отговаря с SYN-ACK но последната стъпка от процеса никога не настъпва, никога не се получава третия пакет ACK. Всеки SYN пакет заема определен ресурс на мишената, следователно при множество SYN пакети изпратени от злодеятеля, машината която е цел на атаката се претоварва и спира да отговаря на всички заявки за връзки, включително и на реалните. Имаме отказ от обслужване. Подправянето на SYN пакети най-често се състои в това, че се подменя адреса на подателя с цел да се прикрие самоличността на атакуващия или да се заобиколи дадена защитна стена, като се използва адрес който е в нейните списъци за разрешение на достъпа. Допълнително тази техника позволява да се прави двойна вреда, защото освен мишената и реалните машини, които са с преправения адрес на подателя получават множество пакети от самата мишена. Всяка полуотворена връзка заема ресурс, а броят на тези връзки е краен. След достигане на този брой, устройството спира комуникациите с потребителите, докато тези отворени връзки не се затворят и изчистят от стека.

SYN атаките са прости атаки, но те все още се използват масово и имат голям успех. Някои от факторите за това са:

SYN пакетите са част от нормалния мрежов трафик и следователно е трудно (по-скоро нелогично) да се филтрират.

За изпращането на SYN пакети не е необходим канал с огромна пропускливост, т.е. всеки нормален потребител има ресурса да извърши такава атака.

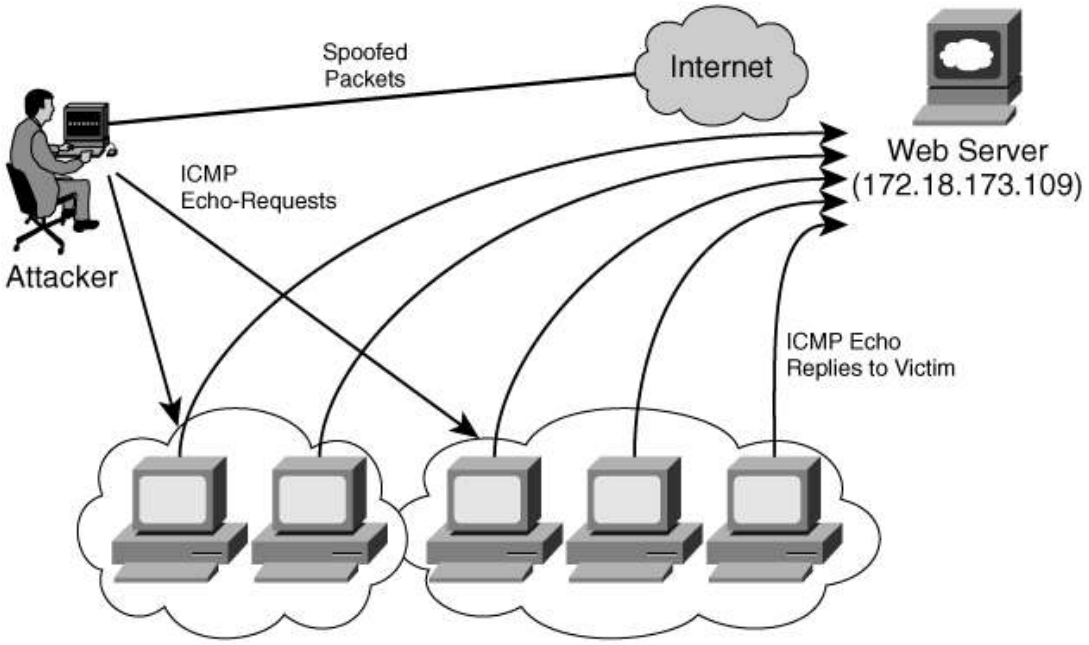
Лесно се променя адреса на подателя поради факта че не се изисква отговор от мишената.

2.1.1.2 Land.c атаки

Изключителност прост и ефективен пример за DoS атака. Атакуващият изпраща множество SYN пакети с еднакви адреси и портове на подателя и получателя. Целта на тази атака е да накара жертвата да изпраща отговор на този пакет сама на себе си. Процесът е цикличен и скоро машината жертва остава без ресурси и спира да предоставя услуги. Хитрото при тази атака е, че атакуващият използва ресурсите на жертвата срещу самата нея. Това е лесен начин за забиване на Windows 2000 (до Service Pack 3) и Windows XP (до Service Pack 2).

2.1.1.3 Smurf атаки

Атакуващия може да „изяде" канала на жертвата и като препраща безполезен трафик към мрежата й. Това е класически пример за Smurf атаки. Два са компонентите изграждащи една такава атака:
Използването на фалшиви Internet Control Message Protocol (ICMP) echo request пакети (ping работи с два определени ICMP пакети, Echo-Request и Echo-Reply)
Маршрутизирането на пакети чрез използването на т.нар. Broadcast адреси (Това са адреси на 2,3 слой, които карат мрежовото устройство да ги разпраща на всичките си портове)
ICMP протоколът по принцип се използва за обработване на грешки (по-скоро да ги съобщава) и да контролира връзката на 3 слой. Друга широка употреба е ping услугата. (Windows ползва ICMP за ping, а Unix, Linux, Cisco IOS, използват UDP пакети на произволен висок порт.)
При Smurf атаките, ICMP echo-request пакети се изпращат към broadcast адреса на отдалечени мрежи с цел да се наруши нормалната работа на мрежата. На **Фиг.2.3** е показа как действа една такава атака.



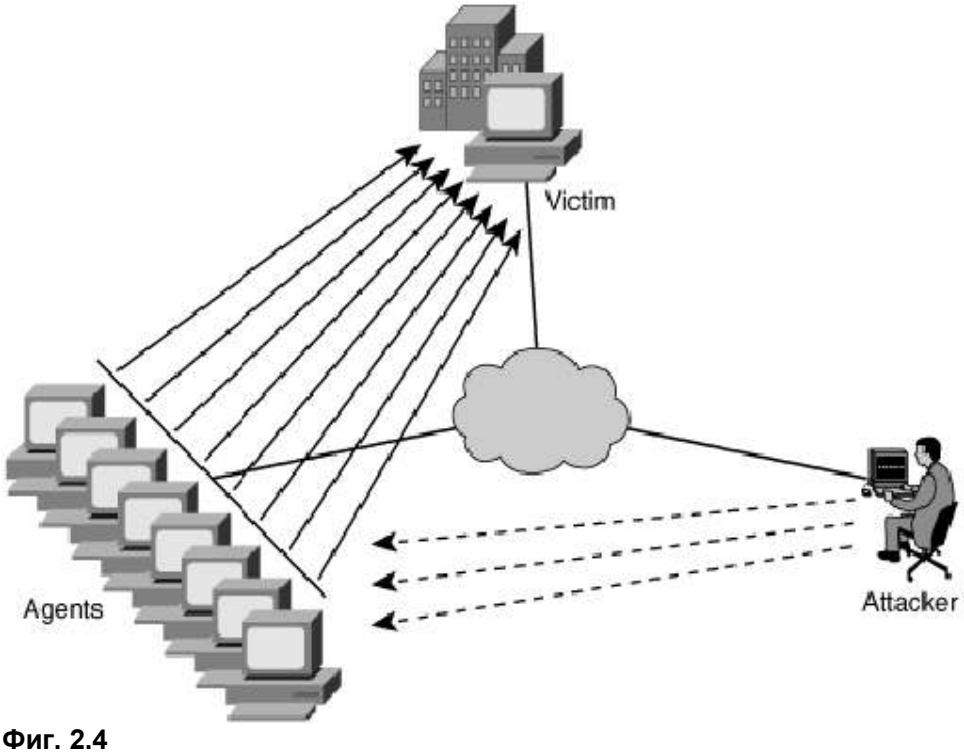
Фиг. 2.3

В Smurf атаките обикновено има атакуващ, посредници, и жертва (в този случай това е уеб сървъра). Нека мрежата в примера е 192.168.1.0 с маска 24 бита. Тогава нейният broadcast адрес ще е 192.168.1.255. Ако изпратим ICMP echo-request пакет към broadcast адреса на тази мрежа, то всички компютри от нея ще изпратят ICMP echo-reply в отговор на адреса на подателя на echo-request пакета. Следователно, за

да е успешна тази атака, тук също трябва да използваме техниката с преправяне на адреса на подателя (spoofing). Тази атака не претоварва жертвата, но запълва целия й канал. Вариация на Smurf атака е Fraggle атаката, но тя използва UDP (user-datagram protocol) вместо ICMP. Fraggle атаките работят като използват CHARGEN и ECHO UDP програми, които заемат UDP портове 19 и 7. Тези две приложения действат на принципа на ICMP ping-а. Те са проектирани да проверяват дали дадени компютри са включени в дадена мрежа. CHARGEN и ECHO изпращат отговор на всеки, който прати трафик на обособените портове. Атакуващият може да се възползва от това, като създаде безкраен цикъл, който да препраща трафик между тези портове.

2.1.2 Разпределени DoS атаки

Този тип атаки изискват много знание от злодеятеля и предварително планиране и подготовка. При тях атакуващият използва различни системи свързани към Internet за да атакува определена жертва и това ги прави много трудни за проследяване и противодействие. Подготовката на атаката се състои в това че злодеятелят предварително разбива защитата на няколко машини в Internet и го поставя под свой контрол като инсталира вреден код. Тези вече компрометирани компютри се наричат агенти, ботове (от роботи) или дори зомбита (заради това че следват сляпо командите на атакуващия). Злодеятелят ползва тези агенти за да извърши координирана едновременна атака от всички ботове към жертвата. Тази атака изяжда канала и мрежовите ресурси на атакувания. Тя е високо ефективна заради това че е координирана (общия ресурс на всички зомбита е много по-голям от този на злодеятеля) и изключително трудна за проследяване. По правило злодеятелят контролира зомбита от обществено достъпна машина (като в интернет кафе или клуб) или през прокси или като използва техниката на подправяне на адреса си. **Фиг. 2.4** пояснява тази вид атаки.



Фиг. 2.4
Легенда: victim = жертва, attacker = злодеятел, agents = зомбита, ботове

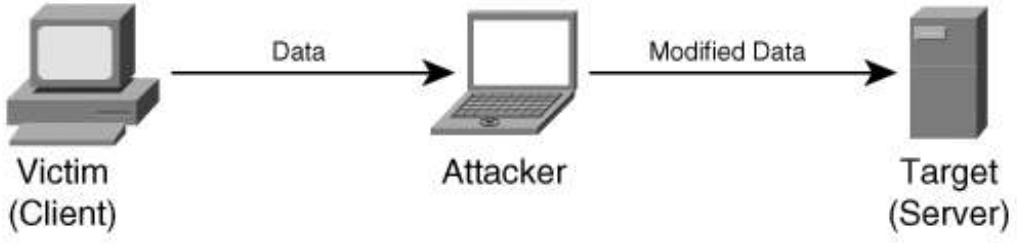
2.1.3 Отвличането на Сесия (Session Hijacking)

При тази атака, злодеятелят пресича вече осъществена сесия или връзка между две системи. Най-често такива атаки се използват при връзки от тип TCP (защото при тях имаме реално изграждане на сесия и следенето и чрез поредни и потвърждаващи номера за разлика от UDP). Целта на този вид атака е злодеятелят да се намърда по средата на сесията и да накара и двата крайни потребителя да разговарят с него, а не помежду си. Тази техника е различна от ip spoofing-а, защото при него е необходимо макар и с подправен адрес да се аутентикираш пред отсрещната страна. При отвличането на сесия двете страни в разговора вече са се аутентикирали. Най-често и тук се ползва spoofing, но далеч не се спира до тук. При повечето стандартни комуникации всякакви защити като стени и аутентикация са преди да бъде установена дадена връзка, след което започват да се предават пакети в четлив вид без защита (това се преодолява чрез частните виртуални мрежи). Ако сесията бъде откраднатa, тогава няма полза от сложния метод на аутентикация и 16 символните пароли.

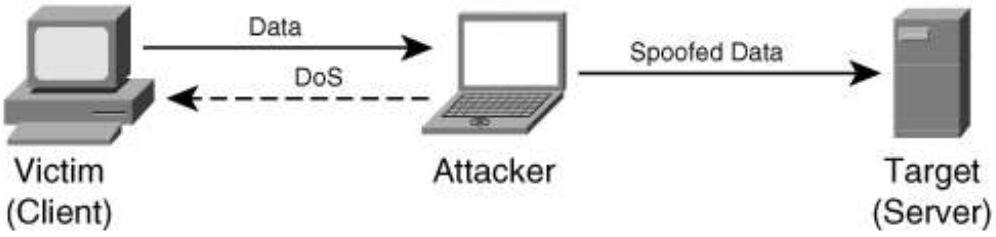
Фиг. 2.5: Обща представа за атака от тип „човек-по-средата”

Известни са два типа отвличания на сесии:
Активен – Отвличаш сесията и я използваш за да пробиеш някаква защита. Ще се спрем по-подробно на нея защото тя е по-сериозна.
Пасивен – Отвличаш сесията и запазваш анонимност, действаш като скрито прокси, което не пречи на комуникацията, а само я подслушва.
Трябва да правим разлика между атака от тип „повтаряне на сесията” и „отвличане на сесията” въпреки че и двете се считат за „човек-по-средата” атаки. При „повтаряне на сесия” ние улавяме пакети, преправяме ги и ги препращаме към мишената. В една истинската атака от типа „отвличане на сесия” ние преправяме адреса си и нагласяме поредните номера (ISN) така че да съвпаднат с тези на първичния инициализатор. Често е необходимо да се извърши и атака от тип DoS срещу инициализатора с цел да го извади от строя, за да можем да заемем мястото му в разговора. **Фиг 2.6 и 2.7** илюстрират разликата между двете техники.

Фиг.2.6. Атака от тип „повтаряне на сесията”



Фиг.2.7. Атака от тип „отвличане на сесията”



Атаките от тип „отвличане на сесията” от своя страна се делят на няколко вида.

- Открито преправяне
- Сляпо преправяне

2.1.3.1 Открито преправяне

При него ние виждаме трафика между потребителя и мишената. Това е най-лесният начин за отвличане на сесия. Изисква се само да се прихванат няколко пакета от разговора. Това обаче може да се окаже проблем в една йерархично подредена, комутирана мрежа. Имаме няколко решения. За първото трябва да имаме достъп до комутатора по пътя на разговора и ако той е Cisco трябва да си осигурим права над него и да конфигурираме Switch Port Analyzer (SPAN) port. Чрез него можем да препращаме трафик от други избрани портове или даже от цели VLAN-и. Ако нямаме достъп до комутатор или няма как да конфигурираме SPAN порт, ни остава второто решение. Чрез използването на програмата за Linux MACOF може да генерираме множество пакети и да напълним таблицата на комутатора така, че да го принудим да broadcast-ва всички пакети. (Не е съвсем ясно колко успешен е този метод срещу Cisco комутатори). Друго решение е да генерираме фалшив ARP пакет, чрез който да излъжем мишената, че другия участник в разговора е на същия порт като нашия (тук говорим за физически порт на комутатор). В крайна сметка, след като се сдобием с така ценните няколко валидни пакета от разговора, ние лесно можем да извлечем от тях липсващото звено за успешното завършване на нашата атака, а именно – поредните и потвърждаващи номера (sequence, acknowledge numbers).

2.1.3.2 Сляпо преправяне

При него няма начин да се сдобием с прихванати пакети. Трябва да отгатнем как са стойностите на SYN и ACK номерата. Важна предпоставка за успешното извършване на такава атака е да се намираме на същия LAN сегмент, на който се намират и мишените. Стъпките са следните:

1. Избираме мишена.
2. Намираме активна сесия, в която тази мишена участва и я следим.
3. Опитваме се да отгатнем seq номерата. При успех пристъпваме натам. Иначе опитваме пак.
4. Извършваме DoS атака срещу единия от участващите в разговора.
5. Отвличаме сесията.
6. По избор, след като си свършим работата с жертвата може да възстановим сесията.

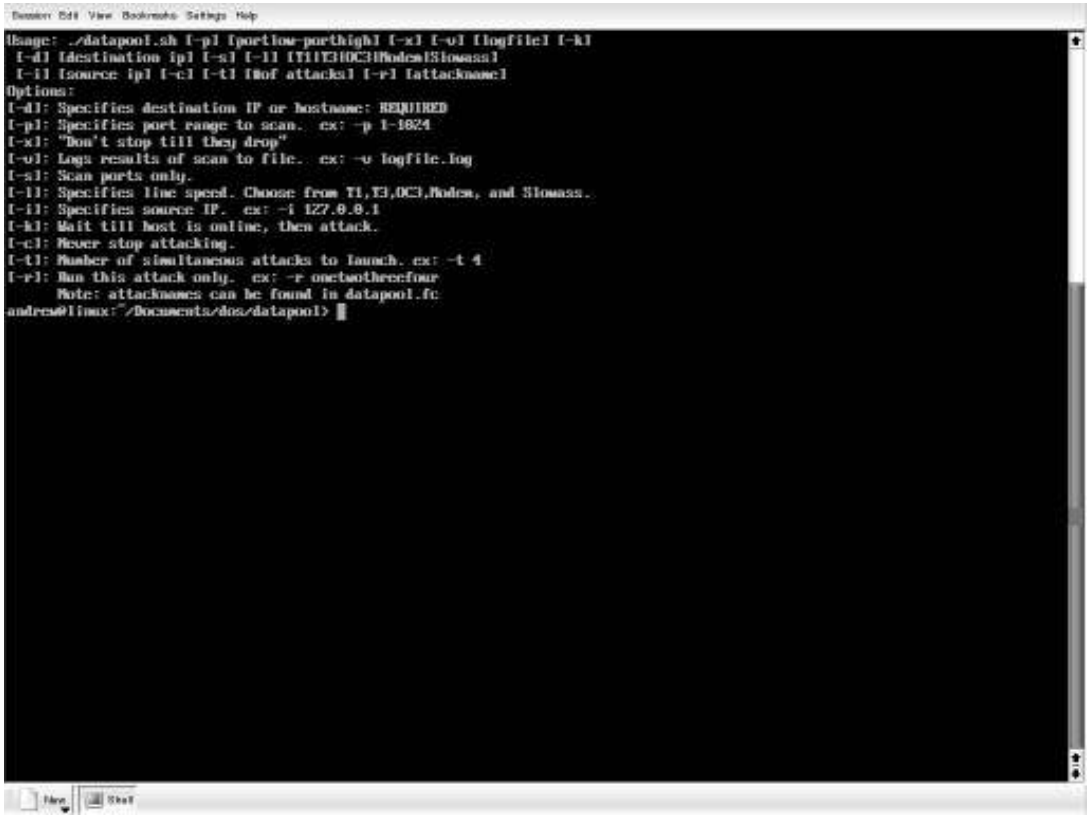
Най-трудната фаза е тази да познаем seq номерата. Те се записват в 32 битово поле в TCP хедъра (следователно са между 1 и 4,294,967,295). Всеки байт се следи, но само последователният номер на първият байт от сегмента се пише в TCP хедъра. Очевидно не можем да разчитаме само на късмет. За радост на атакуващите според RFC 793 номера трябва да бъде увеличаван на всеки 4 микросекунди. Някой от операционните системи не се съобразяват с това и имат свой начин инкрементиране на този номер. При BSD и Linux поредните номера се увеличават с 128000 на всяка

секунда. (Броячът се превърта на всеки 9:32 часа). Още повече ни улеснява факта че на нас не ни трябва да уцелим точно поредния номер, а просто попадението ни да е в текущия TCP прозорец. Пример за TCP прозорец е даден на **Фиг.2.8.**

Фиг.2.8. TCP прозорец

При сляпото отвличане на сесия трябва успешно да отгатнем и поредния номер и големината на прозореца. Въпреки вероятностния характер на тази операция, въоръжени с тези знания имаме шанс, въпрос е само на време докато успеем. Cisco Adaptive Security Appliance, най-новото от Сиско в областта на мрежовата сигурност, предлага решения за всички атаки, описани в тази глава. Например за последната атака, защитната стена подменя ISN и ACK номерата (произлизащите от вътрешните устройства номера са обикновено псевдопроизволни доколкото тези генерирани от ASA са напълно произволни) на всички пакети, които излизат от нея, и по този начин елиминира шансовете за сляпо отвличане на сесия. Целия процес остава прозрачен за крайния клиент.
Инструменти за извършване на атаките:
Популярни инструменти за извършване на DoS атаки са: Datapool, Hgod, Jolt2
Datapool – върви под Linux и поддържа над 100 вида DoS атаки.

Фиг.2.9 показва елементарното меню,с което всеки може да извършва атаки.



Фиг.2.9

Синтаксисът на командите варира, като минималния е да напишем само адрес на получателя (жертвата). Следния ред е показва типична команда, която има за цел да атакува потребител с адрес 192.168.10.10, като се крием зад фалшив адрес 192.168.10.9

#./datapool.sh -d 192.168.10.10 -p 1-1024 -v results.log -l T1 -l 192.168.10.9 -c -t 100

Ключът –v е въведен, за да могат резултатите да се запишат в лог; -l определя скоростта (в случай T1); -c указва програмата да не спира докато мишената е разбита; -t указва на програмата колко едновременни сесии да ползва. За повече сесии се изискват и повече ресурси на атакуващата машина.

Jolt 2 – Работи и под Linux и под Windows. Тя също позволява на атакуващия да скрие адреса си чрез spoofing.

Фиг.2.10 показва снимка с опциите които дава този софтуер.

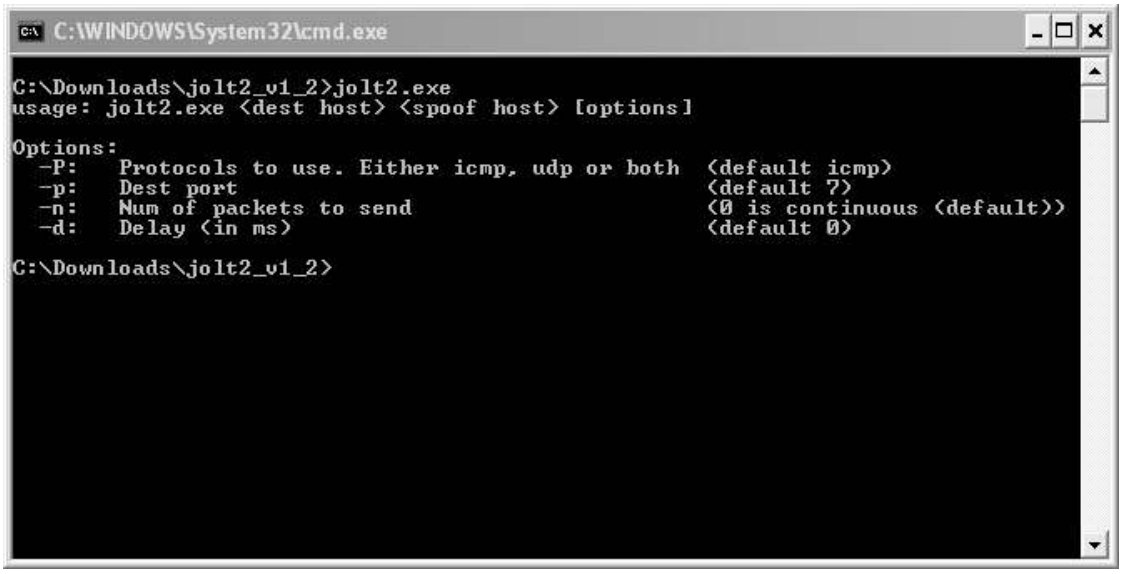
Ключове:

-P : Посочва протокол, чрез който ще се проведе атаката (ICMP, UDP)

-p : Порт на получателя

-n : Брой на пакетите, които ще се изпратят

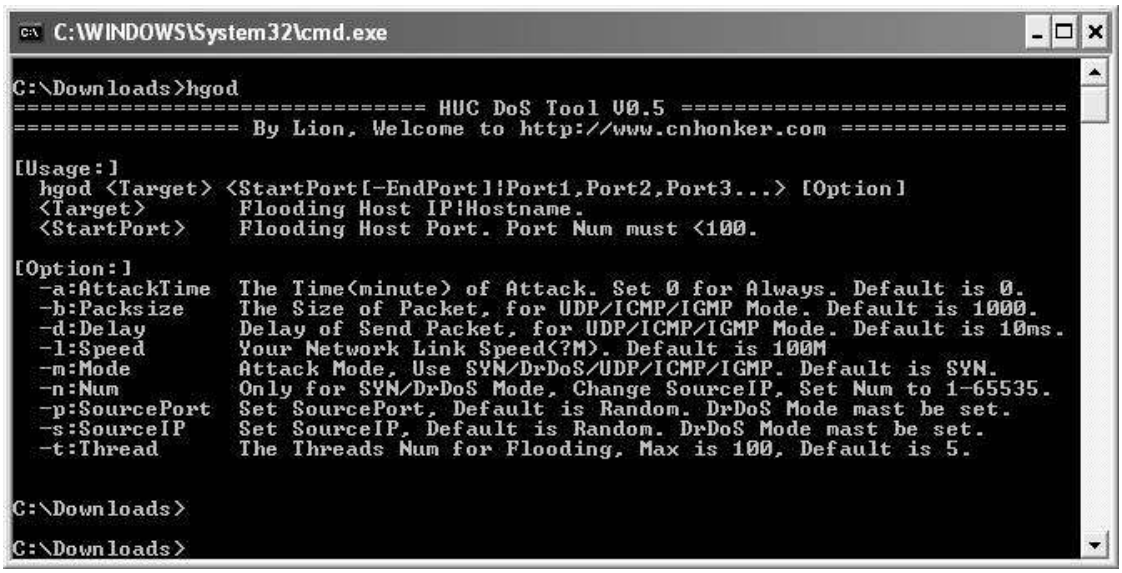
-d : Закъснение между изпратените пакети



Фиг.2.10

Hgod

Hgod е още едно приложение която работи под Windows XP. Позволява подправяне на адреса на подателя. Има възможност да се избира протокол, на който да се основава атаката (TCP/UDP/ICMP/IGMP) и номер на порта (само при UDP). Поддържа множество DoS атаки, но по принцип най-използваната е TCP SYN атаката. На **Фиг.2.11** са показани опциите на тази програма.



Фиг. 2.11

Примерен ред, чрез който може да проведем атака срещу 192.168.10.10 на порт 80 (масово отворен порт заради разпространението на HTTP) като се крием зад адрес 192.168.10.9 е следният:
Hgod 192.168.10.10 80 –s 192.168.10.9

Тази част от главата имаше за цел да покаже нагледно колко е елементарно да се проведат DoS атаки (като това важи и за другите типове атаки). Всеки интелигентен човек с минимални познания в областта на компютрите и мрежите може чрез

използването на тези програми и компютър с достъп до Internet да проведе успешна атака. Това показва необходимостта от мрежова сигурност.
В следващият раздел от настоящата дипломна работа ще разясня един методичен подход за изграждане на добре защитена мрежа, започвайки отдолу и движейки се нагоре в слоевете на OSI модела.

2.2 Избор на устройства и изграждане на защитена мрежа

Изграждането на напълно защитена информационна мрежа е невъзможно поради наличието на една много важна променлива – човешкия фактор. Необходимо е обаче всеки специалист по сигурността да се стреми да осигури максимална сигурност. Мрежовият експерт трябва да може да прецени какви устройства са му нужни за тази цел. Удобен и високо ефективен подход е да се използва OSI модела и да се върви нагоре до слоевете му чак до седмия.

2.2.1 Защита на физическия слой от OSI модела

Тук може да се включи само физическата защита на трасетата и да се ограничи достъпа до устройствата. Ако не се използват наети линии а споделени, необходимо е да се прибегне до технологии от по високите слоеве, за да се осигури защита, примерно частни виртуални мрежи в комбинация с виртуални мрежи на втори слой (VLAN). От изключителна важност е да се ограничи физическият достъп до сървърното помещение. Препоръчително е да се въведе система за оторизиране с помощта на магнитни карти или подобна. Като допълнителна защита трябва да се премахне всякаква възможност за конзолен достъп до устройствата от неоторизирани лица и да се изисква оторизация за администраторите. Трябва да се изгради и подходяща logging система, която точно да записва дата, час и от кой администратор са направени промени, и какви точно са те.

2.2.2 Защита на каналния слой от OSI модела

Съществуват следните видове атаки на този слой:

- Прескачане на VLAN (Virtual Local Area Network)
- Атаки използващи Spanning Tree протокола
- Запълване на MAC (Media Access Control) таблицата
- ARP (Address Resolution Protocol) атаки
- VTP атаки

2.2.2.1 Прескачане на VLAN (Virtual Local Area Network)

VLAN-ите са метод, който сегментира на втори слой мрежата, така се получава разделяне на broadcast домейна. Необходимо е маршрутизиращо устройство, за да може да се пренесе трафик от един VLAN в друг. Това обаче не е сам по себе си гарантиран метод за защита на мрежата. Злонамерен потребител с малко повече умения и знания може лесно да „прескочи” от един VLAN в друг използвайки вратички в DTP (Dynamic Trunking Protocol), т.е да изпраща трафик към мрежи, в който не е оторизиран, а също и да подслушва трафик от тях. Този протокол се използва за да се договарят автоматично trunk връзките между комутаторите. Trunk е връзка, по която се позволява да минава трафика от множество VLAN-и. Това се прави чрез използването на 802.1Q протокола.
Договарянето на връзката се извършва използвайки състоянието на порта според DTP (имаме 5 възможни състояния, описани на таблица 2-1).

Таблица 2-1. DTP състояния

Състояние	Описание
On	Портът е настроен да бъде trunk.
Off	Портът е настроен като порт за достъп (access port) и не е trunk.
Auto	Портът е настроен автоматично да договаря статута си. Ще стане trunk ако порта от другата страна иска да бъде trunk.
Desirable	Като auto, с разлика че портът изпраща активни съобщение че иска да бъде trunk.
Nonegotiate	Портът не слуша никакви DTP пакети и е настроен да бъде trunk. Няма никакви договаряния в случая.

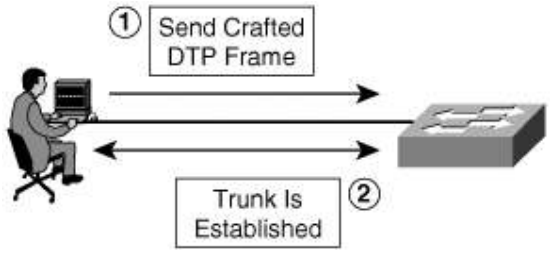
Таблица 2-2 показва какви трябва да бъдат състоянията на двата отсрещни порта за да може да се вдигне trunk линия.

Таблица 2-2. DTP договаряне

Ком1/Ком2	ON	OFF	AUTO	DESIRABLE	NONEGOTIATE
ON	Trunk		Trunk	Trunk	
OFF					
AUTO	Trunk			Trunk	
DESIRABLE	Trunk		Trunk	Trunk	
NONEGOTIATE					Trunk

По принцип повечето мрежови устройства са настроени да пренасят през техните trunk връзки всички VLAN-и. При 802.1Q протокола, който се използва от DTP, четири байта се добавят към Ethernet (frame, втори слой) хедъра и в тях едно от полетата показва този фрейм към кой VLAN принадлежи (другите полета се използват за приоритет, така наречения QoS на втори слой, за контролна информация и други). Това е процедурата, когато фреймът влиза в даден trunk. Когато фрейма напуска trunk и влиза в друг комутатор, 802.1Q хедъра се премахва, CRC сумата на края на фрейма се пресмята пак, и фреймът се връща обратно в нормалния си формат. „Прескачането” от VLAN на друг VLAN се възползва точно от описания механизъм на работа на DTP. При него създаваме фалшиви DTP пакети с които целим да заблудим отсрещния комутатор, който взема компютъра ни за комутатор. Изпращаме DTP съобщение, което казва че ние (преправени като комутатор) искаме тази линия да е trunk. Когато истинския комутатор види това съобщение, при включено автоматично уговаряне на trunk, връзката от нормална става trunk и атаката е осъществена успешно. **Фиг. 2.12** илюстрира този процес

Фиг.2.12. „Прескачане” на VLAN



Друг начин за извършване на тази атака е чрез двойна енкапсулация на пакета (т.е чрез два 802.1Q хедъра), но тя е по-сложна и няма да бъде разглеждана тук. Защитата от този вид атаки не е сложна и винаги трябва да се прави. При Cisco Catalyst сериите комутатори това може да стане чрез следните команди:
Ако искаме порта да е access:
Switch(config-if)#switchport mode access
Конфигурираме даден порт като access port, следователня всякакви DTP пакети получени от такъв порт ще бъдат счетени за анормални и порта се поставя в специален изключен режим.
Ако даден порт трябва да е trunk:
Switch(config-if)#switchport mode nonegotiate

Switch(config-if)#switchport trunk allowed vlans [vlan range]

С първата команда спираме DTP протокола и правим порта trunk без уговаряне. Втората команда е препоръчителна и определя по trunk връзките какви VLAN-и да преминават.

2.2.2.2 Spanning-tree атаки

Spanning Tree Protocol (STP) създава топология на слой 2 от OSI модела, в която да няма цикли. Той прекъсва безкрайните зацикляния на пакети при резервирани (с повече от едно трасе до различни точки) мрежи, като блокира определени портове. Такъв подход за изграждане на мрежите е абсолютно задължителен в съвременните комуникации, където бизнесът не търпи да има прекъсвания. Но зацикляне на пакети води до претоварване на мрежовите устройства и до изяждане на капацитета на връзката.
STP протоколът е задължителен във всяка мрежа с резервирани връзки. Чрез него устройствата си обменят съобщения (BPDU) на всеки две секунди. Всеки комутатор изпраща BPDU съобщение, като в едно от полетата включва своя bridge ID (приоритет на комутатора + най-големия MAC адрес на порт). Комутаторът с най-малкия bridge ID се определя за корен на дървото (root bridge). Целта е в една наглед плоска структура да се създаде йерархия от тип “дърво” и да се избере нейния корен, до който всички устройства, участващи в топологията да има само една действаща връзка. (Тя се определя от различни фактори, на първо място е капацитета на връзката, после MAC адреса на порта). По този начин става невъзможно зацикляне на пакети. По забранените връзки не се движи потребителски трафик но текат BPDU пакети, така че ако активната връзка отпадне, да може да се активира почти моментално резервираната (3-50 сек в зависимост от реализацията на протокола). Даден злонамерен потребител може да се възползва от начина на работа на STP протокола и да причини атака от тип DoS. Това става чрез създаването и изпращането на фалшиви BPDU пакети, твърдящи че потребителят който пред реалните устройства се оприличава като комутатор, има най-нисък bridge ID, в следствие на което може да се излъжат истинските устройства че злосторникът е корена на STP дървото. Така се разваля сегашната структура и се създава нова, в която са възможни зацикляния, който могат да сринат мрежата.
Защита от този тип атаки:

Ефективна защита е използването на BPDU Guard функцията при Cisco Catalyst сериите. BPDU Guard затваря всеки порт предварително конфигуриран с PortFast командата, когато получи каквото и да е BPDU съобщение от него. Командата е следната:
Switch(config)#spanning-tree portfast bpduguard

2.2.2.3 Запълване на MAC (Media Access Control) таблицата

Атаки от този тип не могат да сринат дадена мрежа, но могат да служат като необходима предпоставка за това (използват при вече споменатите атаки от тип „отвличане на сесия"). Те се възползват от основната идея на работа на всеки нормален комутатор. Както знаем, разликата между комутатор и повторител е в това че за разлика от повторителя, комутаторът не изпраща всяко получено съобщение на всичките (освен този от който го е получил) портове, а директно на порта на получателя. Това е възможно чрез употребата на т.нар. MAC таблица, в която се съхраняват връзката между MAC адрес и физически порт.
Механизмът на попълване на таблицата е елементарен, проверява се адреса на подателя на всеки получен пакет, и ако го няма в MAC таблицата, той се попълва като се асоциира с порта, на който е получен пакета. После се проверява адреса на получателя спрямо таблицата и пакета се изпраща на съответния порт. Ако липсва запис за този адрес се привежда в действие механизмът на broadcast-а. При него пакетът се разпраща на всички портове, освен този от който е дошъл.
MAC таблицата се пази в памет от тип кеш (Cache), тук се нарича CAM (content addressable memory). Нормалната големина на паметта е 128 KB и е възможно да бъде препълнена. Тогава комутаторът ще се държи като повторител. Това лесно се прави, като за целта е необходимо даден потребител да изпрати каквито и да са множество пакети, всеки с различен адрес на подател. Достъпна програма за целта е macof. Въпреки че такъв вид атака не може да блокира дадена мрежа, тя може значително да улесни подслушването в нея.

Защита от този тип атаки:
Необходима е употребата на port security (сигурност на портовете). Чрез тази функционалност могат да се ограничат броят, както и точно да се специфицират MAC адресите, които се допускат до даден порт. Ако такъв порт получи пакет с адрес на подателя различен от разрешения, порта автоматично се гаси.
Конфигурацията е на две стъпки:
1) Switch(config)#mac address-table static 0900.0D31.005F vlan 4

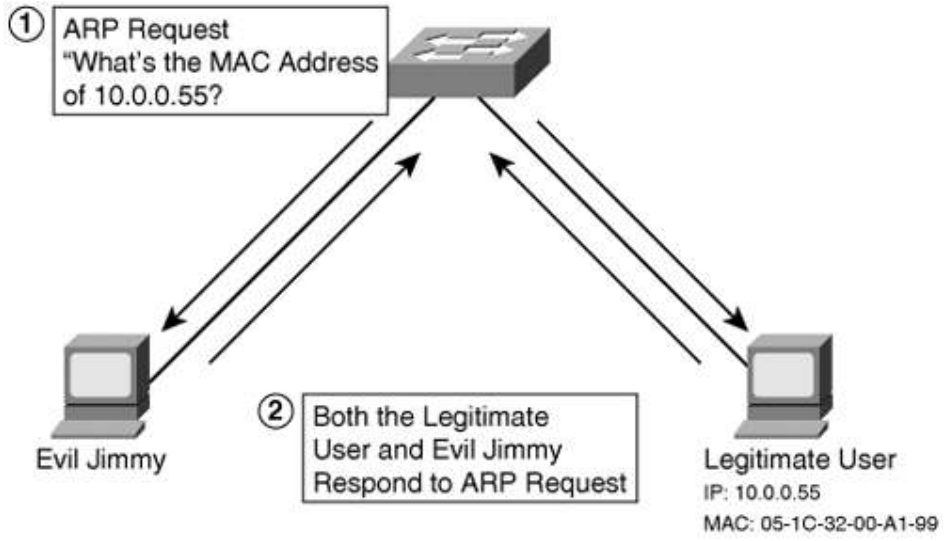
interface fastethernet 0/0
Статично определяне разрешения адрес и VLAN-а. Тази команда задава че само потребител с MAC адрес 09-00-0D-31-00-5F, който принадлени на VLAN 4, може да се вързва към порт fastethernet0/0 .
2) Switch(config)#switchport port-security violation shutdown
В тази стъпка се определя какво да е действието ако бъде засечено такова нарушение. В случая изключваме порта.

2.2.2.4 ARP атаки

ARP атаките също не се използват самостоятелно ,а са често част от друга атака. ARP протоколът дефинира връзката между адреса на мрежовия слой (IP) и този от каналния (MAC). ARP запитвания (requests) се „broadcast-ват", когато даден потребител знае IP адреса, но не и MAC адреса на търсения host. Злонамерен потребител може да преправи ARP отговора (reply) с цел да насочи трафика към определен host да минава през него. Понеже обикновено легитимни потребители също

отвръщат на ARP запитвания, за да е успешна атаката трябва препратения отговор да стигне първи до запитващия.
На **Фиг.2.13** е показан процеса на ARP атаката.

Фиг.2.13. ARP атака



Защитата от този тип атаки е като много добре и ясно се дефинират за всички потребители и комутатори, точно кой порт към кой адрес се асоциира. Командите за това ги показахме при предишната атака (Атака от тип запълване на MAC таблицата)

2.2.2.5 VTP атаки

VLAN Trunking Protocol (VTP) е управляващ протокол, чиято цел е да намали повторението при конфигурирането на големи мрежи. Той служи за синхронизация на броя и имената на VLAN-те в дадена мрежа. Идеята е тези параметри да бъдат въведени само на един комутатор и те автоматично през този протокол да се появят в конфигурациите на всички комутатори в мрежата (VTP domain). При VTP протокола комутаторите могат да работят в три режима – Transparent (прозрачен), Server (сървър), Client (потребител). Промени, нанесени в VLAN конфигурацията на комутатор в режим сървър, моментално се разпространяват по всички други комутатори от тип сървър и потребител, но не и в прозрачните комутатори. За да се следи коя е най-последната версия на VLAN конфигурацията, използва се т.нар. „configuration revision number". При всяка извършена промяна този номер се увеличава с едно.
Злонамерен потребител може да се възползва от този протокол, да се обяви за сървър и да разпространи в мрежата конфигурация на VLAN-и с ревизионен номер по-висок от сегашния, в следствие от което да заличи валидната досегашна конфигурация. Това автоматично кара всички портове да се асоциират с VLAN 1 и така да разруши тази защита. Тази атака често се използва заедно с атака от тип „прескачане" на VLAN, защото е необходимо злодеятелят да се представи като комутатор и да изгради trunk линия.
Защита от този тип атаки:
Две са възможностите:

1) Да се спре VTP протокола, което е неприложимо за големи мрежи
2) Да се създадат пароли чрез който да се защити VTP операцията.

При първият начин всички комутатори се конфигурират като прозрачни и ръчно в тях се описват VLAN информацията.

```
Switch#vlan database
```

```
Switch(vlan)#vtp transparent

Switch(vlan)#vlan 2 name SU
```

Вторият начин е да се въведе парола и всички vtp съобщения които не са с тази парола да бъдат пренебрегвани.

```
Switch(vlan)#vtp password su-s0fia
```

Тук паролата е su-s0fia с нула вместо “o” за по голяма сигурност.

Всички разгледани до тук дупки в сигурността са или свързани с проблеми с недоизпипани протоколи или с протоколи чиято единствена цел е улеснение на администраторите при изграждането на дадена мрежа. Следователно трябва вътрешно да се отнасяме с подозрение и внимание към всичко което улеснява нещата.

Проблеми със сигурността свързани с CDP

CDP протоколът е частен протокол на Cisco Systems, който върви само между Сиско устройства (маршрутизатори и комутатори). Той се използва, за да се събира информация относно адреси на трети слой - платформа, операционна система и други. CDP не поддържа криптиране и няма методи за оторизация на участващите в разговора устройства. Злодеятел може да се престори че е Cisco устройство и да получи информация за другите легални устройства в мрежата. Също така в по-старите версии на Cisco IOS (операционната система) има грешка (бъг – bug), която кара усторйството да блокира при множество получени за кратък период от време CDP пакети. Това може да се използва от всеки злодеятел, който под Linux, използвайки програмата IRPAS, ще бълва пакети с този формат чрез командата.

```
Linux#./cdp -i eth0 -n 100000 -l -1480 -r
```

-i : интерфейс; -n - брой на пакетите; -l : MTU големина; -r – с този ключ се указва CDP пакетите да имат произволни идентификационни номера.
Този проблем със сигурността може да бъде решен по два начина:

1) Ако не ни е необходим CDP протокола можем изцяло да го спрем с:
   ```
   Router(config)#no cdp run
   ```

2) Можем да ограничим интерфейсите, по които да се пускат CDP пакетите:
   ```
   Router(config-if)#no cdp enable
   ```

3) Можем да обновим операционната система на устройството(Cisco IOS) с по-нова,в която е изчистен съответният bug

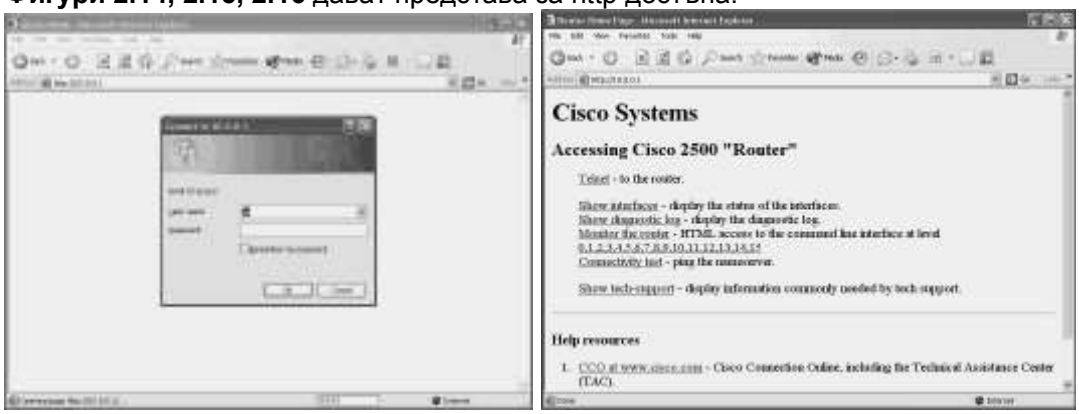
2.2.3 Проблеми със сигурността на мрежовия слой свързани с маршрутизатори

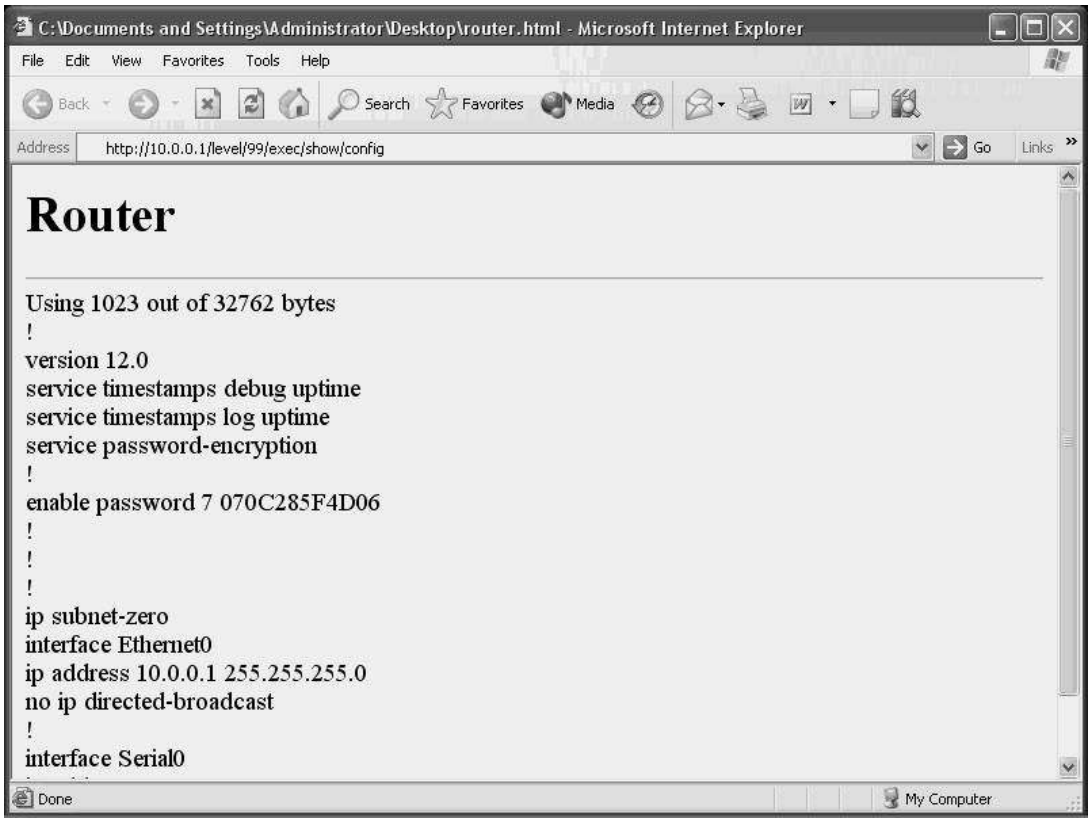
Проблемите на сигурността за мрежовия слой са много поради факта че имаме усложняване на протоколите. Уплътняването на сигурността на мрежовото ниво е от изключителна важност за общата защита на мрежата.

2.2.3.1 Проблеми свързани с сигурността на метода за конфигуриране на устройствата

Повечето мрежови устройства имат няколко начина за конфигуриране. Най-често използваните са: отдалечени терминална връзка (Telnet, SSH), през конзолата,

отдалечено чрез SNMP (simple network management protocol), и през уеб интерфейс използвайки HTTP (напоследък се използва главно HTTPS, secure HTTP, чрез SSL). Използването на чист HTTP (а както и на telnet) не се препоръчва по две причини. Първата е че се отваря порт 80 към устройството, който е предпочитан порт за атаки поради това че масово е отворен, а втората е че някой от по-старите операционни системи на Cisco имат bug, който позволява да се види от неоторизирано лице системната конфигурация. Това е съществен недостатък, защото въоръжен с хеша от паролата можем да видим самата парола чрез определено приложение.
Следният ред показва конфигурацията
http://ip address/level/99/exec/show/config
Фигури 2.14, 2.15, 2.16 дават представа за http достъпа.





На **Фиг.2.16** сме използвали bug-а в ОС на маршрутизатора и сме се сдобили с конфигурацията. Виждаме, че е използван MD5 хеш алгоритъм (от командите enable password, enable password-encryption) и самия хеш код. MD5 не можем да разкодиране лесно, но благодарение на това че Cisco ползва (в по-старите IOSи)

едни и същи променливи за MD5 алгоритъма, е възможно да се направи таблица на съответствията между паролите и хеша им. Подобна програма е Boson GetPass! и на **Фиг.2.17** се вижда колко лесно се намира паролата.

Фиг.2.17

Този проблем лесно се решава, като се забранява използването на Telnet и HTTP
Router(config)#no ip http server
Или чрез ограничаване на потребителите които имат достъп до него:
Router(config)#access-list 1 permit host 10.0.0.5

Router(config)#ip http server 1
Трябва също винаги да се ползва последната операционна система.
Възможно е да използваме също и външен сървър за автентикация (RADIUS или TACACS+). Примерна конфигурация може да е:
Router(config)#aaa new-model

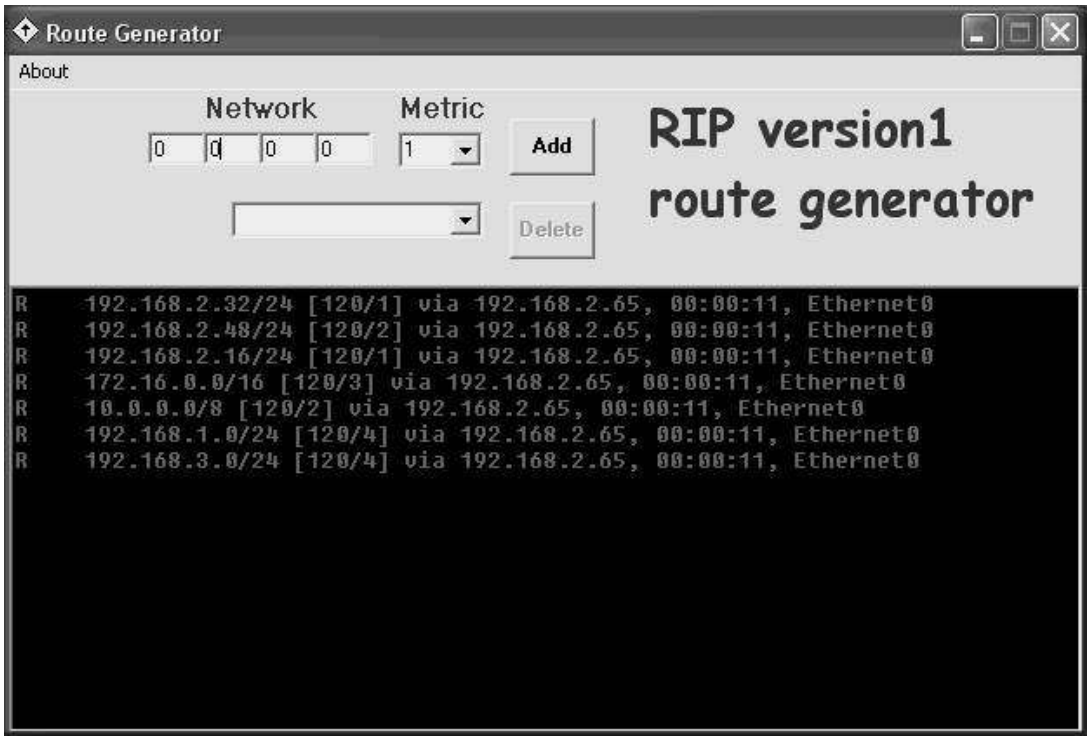
Router(config)#aaa authentication login default tacacs+

Router(config)#tacacs-server host 10.0.0.5

Създаваме AAA (authorization, authentication, accounting) модел,който се ползва услугите на TACACS+ сървър на адрес 10.0.0.5 който проверя валидността на потребителя и го допуска или не до устройството.

2.2.3.2 Проблеми свързани с инжектирането на зловредни маршрути

Някои от по-старите маршрутизиращи протоколи (RIP v1) не поддържат оторизация на съобщенията, чрез които се разменят маршрути и се поддържа маршрутизиращата таблица. Това е потенциален проблем, защото злонамерен вътрешен потребител може да инжектира неправилни маршрути и това до доведе до невъзможност за достъп до определени мрежи. Програма, която може да „отрови” маршрутизиращата таблица за RIP v1, е показа на Фиг.2.18.



Фиг.2.18

Всички протоколи могат да бъдат лъгани по този начин, за това винаги се препоръчва като защита от това да бъде използвана аутентикация. При RIP v2 това става със следните команди.
Първо е необходимо да създаден „ключодържател" (key-chain) и да посочим парола.

```
Router(config)#key chain MYCHAIN
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string cisco
```

След това трябва да асоцииране вече създадения ключодържател с интерфейс на който работи RIP и да включим MD5 автентикацията.

```
Router(config)#interface fastethernet 0/0
Router(config-if)#ip rip authentication key-chain MYCHAIN
Router(config-if)#ip rip authentication mode MD5
Router(config)#interface serial 0/0
Router(config-if)#ip rip authentication key-chain MYCHAIN
Router(config-if)#ip rip authentication mode MD5
```

2.2.4 Проблеми със сигурността на слоеве от транспортния до приложния

Към тази подточка се отнасят всички описани досега видове атаки.

2.2.4.1 Защита от DoS атаки

Истинският ключ към защитата от DoS атаки е предпазливостта. Опитът показва, че като намаляваме „площта", която е податлива на атака, намалява и шанса за успешното провеждане на такава. Като правило обаче няма напълно защитена

система. В реалността ние създаваме една подредена и йерархична система от защити и се надяваме тя да е достатъчна. Основен списък от неща, които системните и мрежови администратори трябва да направят, за да намалят шанса за успешна атака е следния:

- Системите винаги трябва да са с последните надграждания (upgrades - ъпгрейди) и най-нов софтуер
- Винаги предлагай само услугите, които са необходими и нищо повече
- Използвай защитни стени
- Използвай системи за засичане на неоторизиран достъп
- Инсталирай антивирусни програми
- Спирай ICMP протокола между маршрутизаторите и защитните стени

2.2.4.1.1 Повишаване на устойчивостта на мрежата спрямо DoS атаки (Hardening)

Чрез повишаване на устойчивостта на мрежовите устройства и приложения се намалява шанса да станем жертва на атака. Тази задача може да се раздели условно на две части:

- Мрежова устойчивост
- Програмна устойчивост

Мрежова устойчивост

Мрежови устройства като защитните стени предотвратяват проникването на нежелан трафик в мрежата и тяхната инсталация е от голяма важност. Защитните стени са създадени за да бъдат сигурни и винаги помагат, но въпреки това всеки мрежови администратор трябва винаги да е в течение с най-новите техники за повишаване на устойчивостта на мрежата.
Първичната задача на маршрутизаторите е да прокарват трафика през мрежата, но изпълнявайки тази задача те могат несъзнателно да подпомагат DoS и дори DDoS атаки ако не ги конфигурираме правилно. Само устройство което маршрутизира трафик не е достатъчно за защитата на дадена мрежа, необходими са защитни стени. Като най-основно правило, винаги трябва да започваме да изграждаме сигурността в мрежата ни чрез прилагането на списъци за контрол на достъпа на външния ни интерфейс, за да спрем възможно преправяне на адреси, което е масова практика при всяка атака. Необходимо е да се **контролират не само външните IP адреси, които имат достъп до мрежата, но и IP адресите на подателите**, които излизат от нея. Ако това правило се спазваше масово, DoS атаките щяха главоломно да намалеят, поради факта че много бързо всеки мрежов администратор ще засече от къде идва атаката, ще спре източника и ще уведоми тамошния администратор. Също така е необходимо да се спират от излизане в Internet пакети със запазени адреси от тип multicast (мрежа D) или адреси дефинирани в RFC1918 (частни адреси). Една примерен списък за контрол на достъпа, която трябва да постави на всеки изходящ интерфейс в посока навън за Софийският Университет трябва да е:

```
access-list 100 deny ip 0.0.0.0          0.255.255.255    any
access-list 100 deny ip 10.0.0.0         0.255.255.255    any
access-list 100 deny ip 127.0.0.0        0.255.255.255    any
access-list 100 deny ip 169.254.0.0      0.0.255.255      any
access-list 100 deny ip 172.16.0.0       0.15.255.255     any
access-list 100 deny ip 192.0.2.0        0.0.0.255        any
access-list 100 deny ip 192.168.0.0      0.0.255.255      any
access-list 100 deny ip 224.0.0.0        15.255.255.255   any
access-list 100 deny ip 240.0.0.0        7.255.255.255    any
access-list 100 deny ip 248.0.0.0        7.255.255.255    any
```

```
access-list 100 deny ip 255.255.255.255  0.0.0.0          any
!Дотук беше стандартната част, сега ще опишем мрежите на СУ

access-list 100 permit ip 62.44.96.0 0.0.224.255

!Позволяваме изходящите пакети от мрежата да СУ да напускат интерфейса САМО ако са с публичните си адреси 62.44.96.0/19, това премахва шанса някой да извърши DoS атака от тази мрежа.
```

В дадения пример това е списък за контрол на достъпа в защитна стена, конфигурирана на маршрутизатор, и затова са използвани wildcard маски. При хардуерната защитна стена се използват нормални маски. Подобен списък за контрол на достъпа, но този път с краен ред permit ip any any, е необходимо да бъде сложен на изходящият интерфейс и в посока навътре.

Защита от атаки от land.c тип

Тази атака, както вече споменах в главата описваща мрежовите атаки, представлява ping с еднакви адрес и портове в полето за подател и получател (адреса е този на жертвата разбира се). За примера използваме постановка при която имаме адрес на външния интерфейс x.x.x.x. Тогава списъкът за контрол на достъпа трябва да изглежда така:

```
access-list 101 deny host ip 10.0.0.1 any

access-list 101 permit ip any any

interface fastethernet 0/0

 ip access-group 101 in
```

Следващата стъпка е да забраним насочените broadcast-и (directed broadcast) през мрежата ни. Това предотвратява атаки от тип Smurf и Fraggle. На Cisco маршрутизатор това се прави със следната команда:

```
no ip directed-broadcast
```

Един от сигурните начина да повишим устойчивостта на нашата мрежа спрямо DoS атаки е да **спрем изцяло ICMP** трафика. Понякога обаче това не е възможно. Тогава е необходимо да ограничим така че да не запълним капацитета и ресурсите на мрежата. Със следващите команди показвам как може да ограничим ICMP трафика така че да не заема повече от 128 килобита. Това се прави че използването на QoS.

```
interface fastethernet 0/0
 service-policy input ICMP-RATE-LIMIT
ip access-list extended ICMP-ACL
 permit icmp any any
class-map match-all ICMP-CLASS
 match access-group name ICMP-ACL
policy-map ICMP-RATE-LIMIT
 class ICMP-CLASS
  police cir 128000 bc 1000 be 1000 //граница 128000к, марж нагоре/надолу 1000к
   conform-action transmit
   exceed-action drop
```

В този пример създаваме списък за контрол на достъпа, който дефинира желания трафик за даден клас, след което прилагаме класа към даден policy-map. Последната стъпка е да приложим policy-map към даден интерфейс чрез използване на service-policy командата.

Трябва да имаме предвид, че не всички DoS атаки използват ICMP, често използван е и TCP. В следващия пример ще опиша как да **намалим въздействието на TCP SYN атаката чрез използването на маршрутизатори** (за защитни стени имаме вграден друг изключително интересен механизъм).

ip tcp intercept mode intercept

ip tcp intercept list 100

access-list 100 permit ip any 10.0.0.0 0.255.255.255

! Контролният списък се използва за да дефинира за коя мрежа да се включва този режим на прихващане.

Програмна устойчивост

В този термин се включват не само нормалните потребителски програми, но също и операционните системи, под които те вървят. Всяка програма има bug-ове. Затова непрекъснато биват изкарвани обновявания (updates – ъпдейти), с които се целят „закърпване" на дупките в сигурността. Това, което трябва да има предвид всеки потребител, е, че винаги трябва да ползва програми от сигурни фирми и програми с отворен код. Да си ги набавя от сигурни места (най-хубаво от официалния сайт), да избягва използването на shareware програми (повечето съдържат скриптове за шпиониране), и задължително ОС да му е с всички последни ъпдейти. Във връзка с DoS атаките трябва да имаме предвид, че е добре да държим в работен режим колкото се може по-малко програми повечето от тях създават сокети (това е комбинация от IP адрес на подадел и порт) и ги държат отворени, което създава „дупки" в защитната стена, освен това колко по-малко общ на брой програми, толкова по-малко потенциални проблеми със сигурността в следствие на bug-ове може да има.
За борба с DoS атаките е препоръчително освен вече взетите мерки за повишаване на устойчивостта на системата да се реализират и системи за да засичане на неоторизиран достъп (IDS/IPS).

2.2.4.1.2 Системи за засичане / предпазване от неоторизиран достъп (Intrusion Detection / Prevention Systems)

Чрез тях вероятността за засичане на DoS/DDoS атаки нараства значително. Засичането на атаката е предпоставка за моментално взимане на мерки и навременна реакция с цел предотвратяване на атаката. Освен това чрез използването на такива системи могат лесно да се изолират слабите места в мрежата и се пристъпи към тяхното подсилване. Системите за предпазване от неоторизиран достъп могат и сами да взимат автоматизирани решения относно моменталното противодействие на атаките. Това става като те изпращат определени (обикновено блокиращи) команди към дадено предварително дефинирано мрежово устройство (най-често хардуерна защитна стена или защитна стена интегрирана в маршрутизатор).
Често DoS атаките са съпроводени с характерни особености, които помагат за тяхното навременно откриване. Това са:

- Ненормално натоварване на мрежата
- Високо натоварване на централните процесори на системите в мрежата
- Липсата на отговор от дадена система
- Честото и необяснимо забиване на системи

Понякога обаче различните DoS атаки трудно могат да се усетят на време и могат да доведат до значителни загуби. Това не бива да се допуска и всяка компания която работи с поверителна информация, преводи на пари по мрежата, или предлага критична услуга трябва да използва поне един или най-добре всички от следните техники за повишаване на устойчивостта и навременно откриване на DoS атаки.

- Защитни стени
- Системи за засичане на неоторизиран достъп при потребителя
- Системи за засичане на неоторизиран достъп във мрежата – чрез използването на сигнатури и аномалии

2.2.4.1.2.1 Системи за засичане на неоторизиран достъп при потребителя

Такъв тип системи както и персоналните защитни стени подпомагат засичането на различен вид атаки, като наблюдават и блокират нежеланите пакети. Проблема при тях е скалируемостта. Дори в една средно голяма мрежа от 100-1000 компютъра е необходим голям екип администратори за да може тези системи да бъдат инсталирани и поддържани правилно. За това тяхната употреба е ограничена предимно до сървъри в демилиратизираната зона.

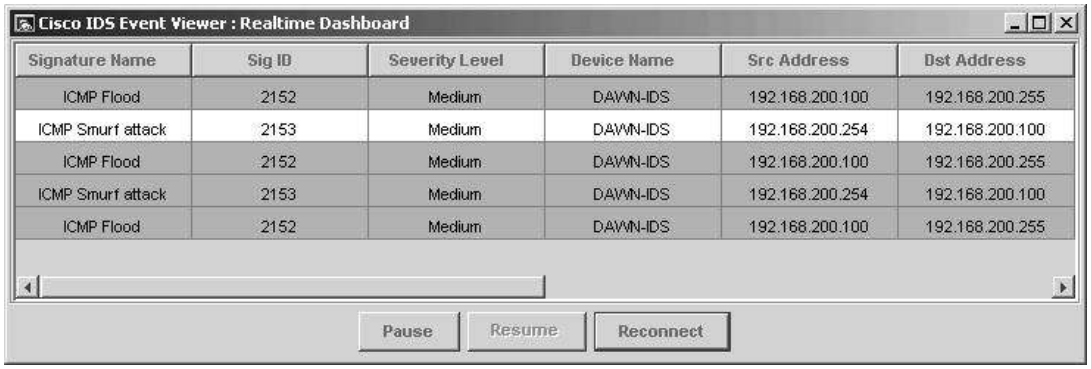
2.2.4.1.2.2 Системи за засичане на неоторизиран достъп във мрежата основаващи се на сигнатури.

Чрез тях ние имаме възможността да анализираме трафика по мрежата и да го преглеждаме за каквито и да са атаки. Хакери от типа „новаци със скриптове" (script newbie's) нямат шанс срещу такива системи, защото те използват широко достъпни и известни (както и на производителите на системи за сигурност) програми за които лесно би могла да се създаде сигнатура. Cisco IDS 4200 серията сензори имат вградени множество сигнатури за различни типове атаки. На **Фиг.2.19** е показа алармата която се показва когато някой използвайки Hgod се опита да осъществи TCP SYN атака.

Фиг. 2.19

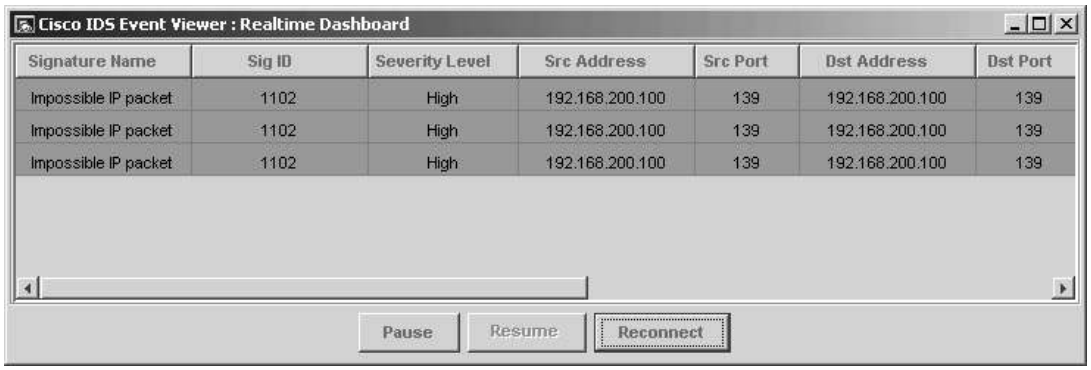
В следващия пример злонамереният потребител използва програма, чрез която преправя пакетите и извършва ICMP Smurf атака директно към broadcast адреса на дадена мрежа (192.168.200.255). IDS, използвайки две сигнатури, засича ICMP Flood и Smurf атаките, както е показано на **Фиг.2.20**.

Фиг.2.20. ICMP Smurf, Flood атаки

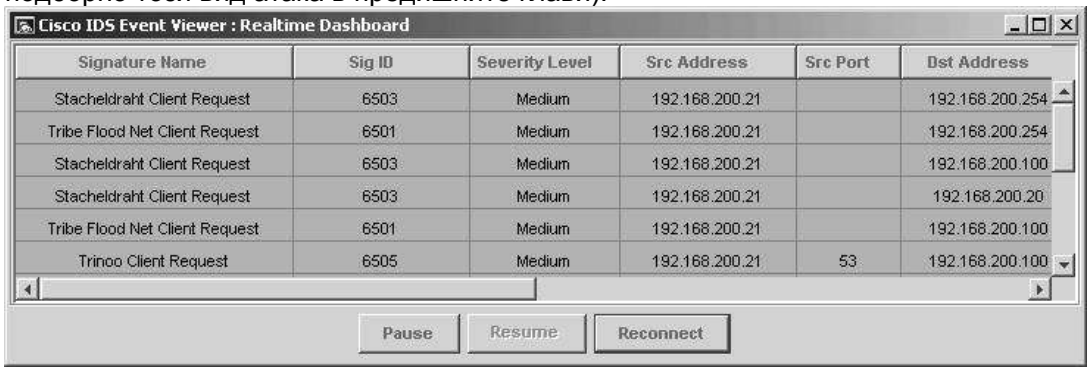


Следващият пример показва алармата, която се получава при засичането на land.c атака. IDS системата веднага улавя пакета чрез сигнатура 1102 „Невъзможен пакет”. **Фиг.2.21** показва това.

Фиг.2.21

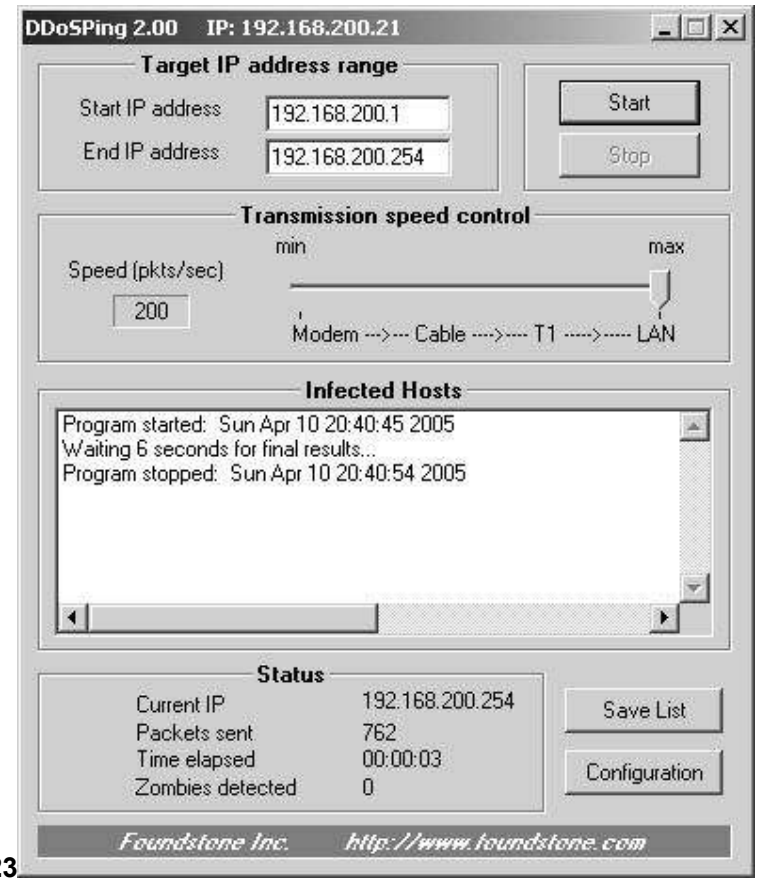


В този пример ще покажа засичането на атака извършена с едни от най-известните програми за извършване на DDoS атаки: Stacheldraht, Tribe Flood Network, и Trinoo. Чрез тези програми преди време бяха „съборени” няколко големи уеб страници. На **Фиг.2.22** е показана комуникацията между атакуващият и неговите зомбита (описах подборно този вид атака в предишните глави).



Фиг.2.22

Добър начин на предотвратяване на атака DDoS е да проверяваме редовно мрежата си за зомбита. Това е лесно да се направи поради факта че повечето зомбита слушат на определени портове за инструкции от атакуващия. Програма чрез която се откриват зомбита е DDoSPing от Foundstone. На **Фиг.2.23** е показан управляващият прозорец на DDoSPing и как той сканира мрежата проверявайки за типичните черти на компютри зомбита.



Фиг.2.23

2.2.4.1.2.3 Системи за засичане на неоторизиран достъп във мрежата основаващи се на аномалии

Въпреки че системите на основа на сигнатура са ефективни срещу добре известни типове атаки и програмите използвани за тяхното извършване, те нямат шанс срещу най-новите атаки (zero-day attacks). Точно за такъв тип атака са създадени системите на принципа на аномалиите. Създадени е малко силна дума, защото те още са в процес на обработка но идеята е на лице, а вече има и изпълнения (Cisco Traffic Anomaly Detector XT). Принципът на действие на системи от този тип е засичането на мрежовия трафик, който рязко се отклонява от нормалния. Например, ако значителен брой UDP запитвания идват от един потребител, това е аномалия и се включва аларма.
Обикновено тези системи вървят ръка за ръка с Cisco Guard XT. Идеята е при откриването на аномалия целият трафик се пренасочва към Guard XT устройството, което чрез използването на сложни алгоритми се опитва да отдели и пропусне само стандартния трафик, всичко подозрително се спира.
Описаните устройства са много скъпи, трудни за инсталация и изискват квалифициран обслужващ персонал, но понякога вредата от дадена атака може да излезе много по-скъпа. Затова всяка компания трябва да е наясно с това колко ще им струва реализацията на дадена система за сигурност, а също и колко ще струва, ако дадена услуга спре да работи, мрежата се срине или чувствителна информация (например като лична информация на потребители, номера на кредитни карти, или технологичен шпионаж) бъде откраднатa. Снабдени с тези данни компаниите и организациите трябва сами да преценят.

Глава III. Одит на сигурността в мрежата на СУ

3.1 Цели на одита и за кого е предназначен той

Основните цели на одита на сигурността на мрежата на СУ са:

1. Да се провери дали са спазени съществуващите политики за сигурност, стандарти, препоръки и процедури;
2. Да се определи ефективността на текущите политики и да се попълнят неточностите в тях;
3. Да се открият всякакви съществуващи уязвимости, които могат да бъдат използвани както от външни лица, така и от оторизирани вътрешни с право на достъп;
4. Да се провери дали извършеният контрол на сигурността при различни възникнали проблеми е съответствал поне с минимума изисквания по сигурността;
5. Да се дадат препоръки и план за прилагане на евентуални промени и подобрения.

Този документ,както и резултатите и препоръките от него биха били полезни на:

- Отговорният за мрежата персонал на Софийският Университет - както за вътрешната, така и за опорната мрежа;
- Всички потребители, които имат или ще имат достъп до мрежата;
- Управленският екип, който одобрява евентуалните промени по политиката за сигурност, както и следи за нейното разпространяване и спазване.

Преди да започнем извършването на одита, приемаме,че за одиторите важат следните правила:

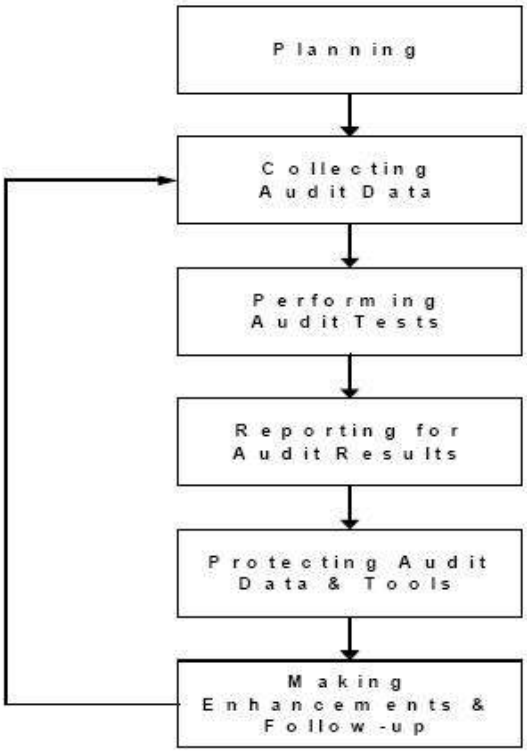
1. Притежават необходимите знания за извършването му;
2. Разбират много добре влиянието и действието на всеки инструмент, който използват, както и евентуалното му въздействие върху потребителите и системите;
3. Получили са писмено разрешение за извършването на този одит;
4. Ще документират всеки тест, който е проведен, независимо от това дали е успешен или не;
5. Сигурни са, че тестовете, които провеждат са в съответствие с поставената задача.

3.2 Основни стъпки

Основните стъпки, по които ще се извърши одита, са: (**Фиг 3.1**)

- Планиране
- Събиране на данни за одита
- Извършване на одит тестовете
- Изготвяне на отчет за резултатите от одита

- Запазване на данните, върху които е извършена оценката и средствата, използвани за това.
- Извършване на подобренията и допълнителна работа.



Фиг.3.1 Основните стъпки при одита

3.3. Обхват на одита

Обхвата на одита трябва да бъде ясно определен (в случая от поставената задача):

- Обща сигурност на вътрешната мрежа;
- Сигурност при връзките с Интернет;
- Сигурност на мрежовият достъп до най-важните мрежови системи, съответно и услугите, които те предоставят (e-mail, web, file servers);
- Защита на мрежовите компоненти – защитни стени, маршрутизатори, комутатори;
- Обща сигурност на техническите помещения

Извън целите и компетентността на този одит са:

- *Сигурността при крайните устройства – работни станции,IP телефони и други потребителски устройства, свързани в мрежата*
- *Сигурността на най-важните сървъри и услугите, които те предоставят сами по себе си;*
- *Предоставянето на мрежови услуги като активна директория (Active directory), пощенски услуги,отдалечен достъп (RAS)*

3.4 Последващи действия след извършването на одита.

След извършването на одита най-голямата полза от него е не в самите препоръки, които ще се направят, а в ефективното им прилагане. Нужно е да се спазва следния цикъл с цел правилното прилагане на препоръките: (**Фиг 4.1**)

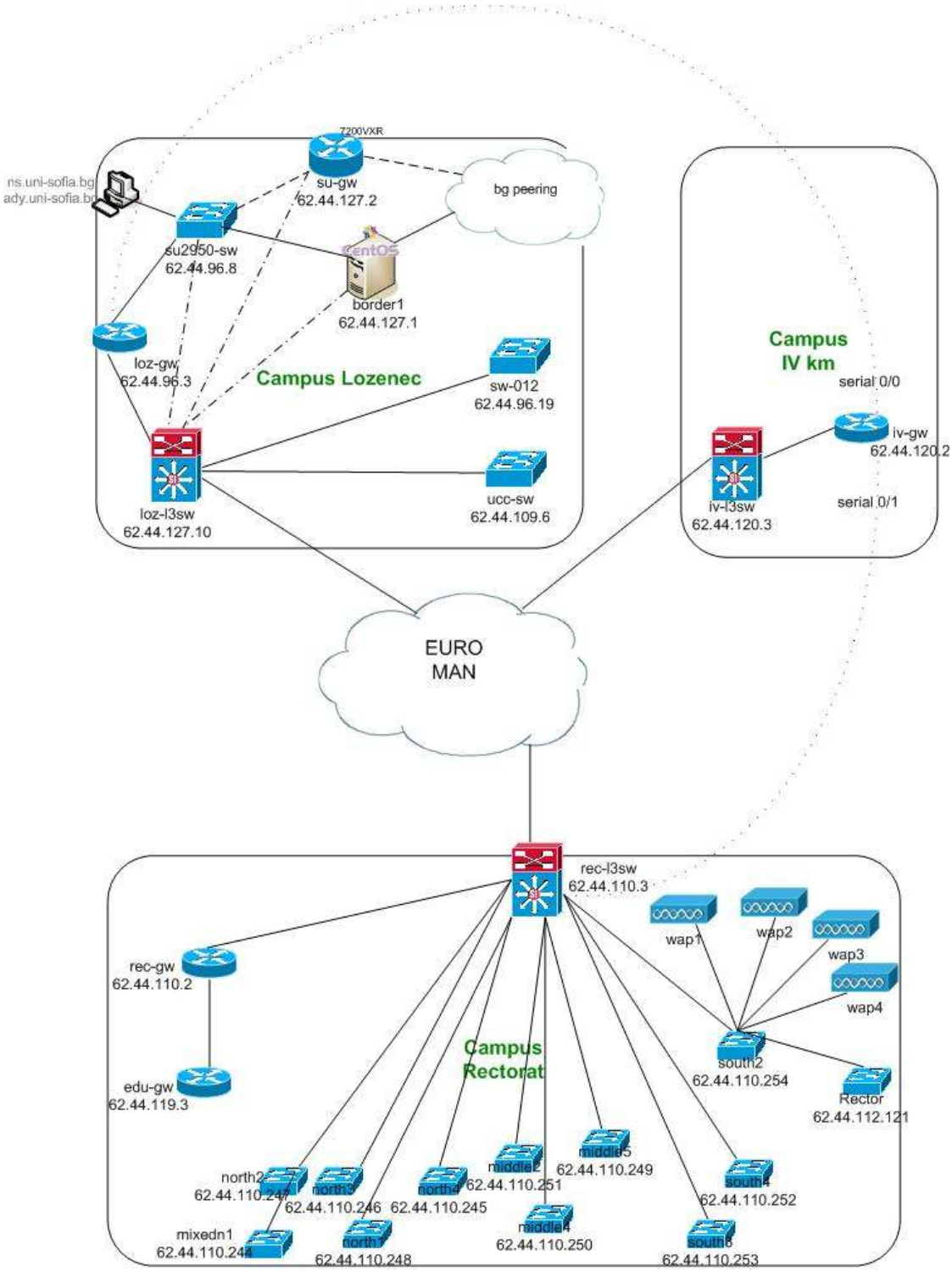
Фиг.4.1 Нужните действия за ефективно прилагане на препоръките от одита.

3.5 Общо описание на мрежата и логически дизайн

При изграждането на мрежата на Софийския университет е използвано главно комуникационно оборудване на Сиско, освен тях няколко HP устройства и Linux (CentOs базирани) сървъри, които играят ролята на маршрутизатори. Ethernet мрежата представлява смесена структура, тип звезда, изградена от 5 броя Cisco маршрутизатори, Linux базирани сървъри, 20 Cisco (HP) комутатора, 4 точки за безжичен достъп (wireless access point), които са разположени в следните три възела (PoP - Point of Presence): Лозенец, Ректорат и IV-ти километър. (За удобство за напред ще ги наричаме съответно Loz, Rec и IV).

Физическата топология на частта от мрежата на Софийския университет, върху която ще се съсредоточи одита, е тип звезда, в центъра на която можем да поставим високоскоростната MAN мрежа (градска мрежа, базирана на технологията Етернет, реализарана върху оптическа преносна среда) на „София Комюникейшънс”. На **Фиг.3.2** е дадена логическата топология на мрежата:

Фиг. 3.2.Логическа топология на СУ



3.6 Детайлно разглеждане на отделните мрежови устройства

В долната таблица са описани версията на софтуера на комутаторите (маршрутизаторите) за всеки възел от мрежата, който се използва в момента.

PoP	Име на възел	IP address	Platform	IOS	
Loz	**Border2**	62.44.127.2	cisco7204VXR	7200 Software (C7200-IS-M), Version 12.3(2)T	
Loz	**loz-gw**	62.44.96.238	cisco7204VXR	7200 Software (C7200-IS-M), Version 12.3(2)T	
Loz	**loz-l3sw**	62.44.127.10	Catalyst 3550-24	C3550 Software (C3550-I5Q3L2-M), Version 12.1(14)EA1	
Loz	**swi_008**	62.44.96.19	Catalyst 2950-24	C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA7	
Loz	**su-backbone-sw**	62.44.96.8	Catalyst 2950-24	C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA7	
Loz	**ucc-sw**	62.44.109.6	Catalyst 2950-24	C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA7	
Rec	**middle2-sw**	62.44.110.251	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**middle4-sw**	62.44.110.250	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**middle5-sw**	62.44.110.249	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**mixedn1-sw**	62.44.110.244	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**north1-sw**	62.44.110.248	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**north2-sw**	62.44.110.247	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**north3-sw**	62.44.110.246	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**north4-sw**	62.44.110.245	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**rector-sw**	62.44.112.121	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**south2-sw**	62.44.110.254	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	

Rec	**south3-sw**	62.44.110.253	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**south4-sw**	62.44.110.252	Catalyst 2950-24	C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA1	
Rec	**rec-gw**	62.44.110.2	Cisco 2500	2500 Software (C2500-I-L), Version 12.0(14)	
Rec	**rec-l3sw**	62.44.110.3	Catalyst 3550-24	C3550 Software (C3550-I5Q3L2-M), Version 12.1(14)EA1	
Rec	**wap4**	62.44.112.125	ciscoAIRAP1210	C1200 Software (C1200-K9W7-M), Version 12.2(15)JA	
IVkm	**iv-l3sw**	62.44.120.3	Catalyst 3550-24	C3550 Software (C3550-I5Q3L2-M), Version 12.1(14)EA1	
IVkm	**iv-gw**	62.44.120.2	Cisco 4500	4500 Software (C4500-P-M), Version 11.1(18.1)	
IVkm	**IV-bl1_sw**	62.44.120.241	HP J4900B ProCurve Switch 2626	HP J4900B , revision H.08.60	

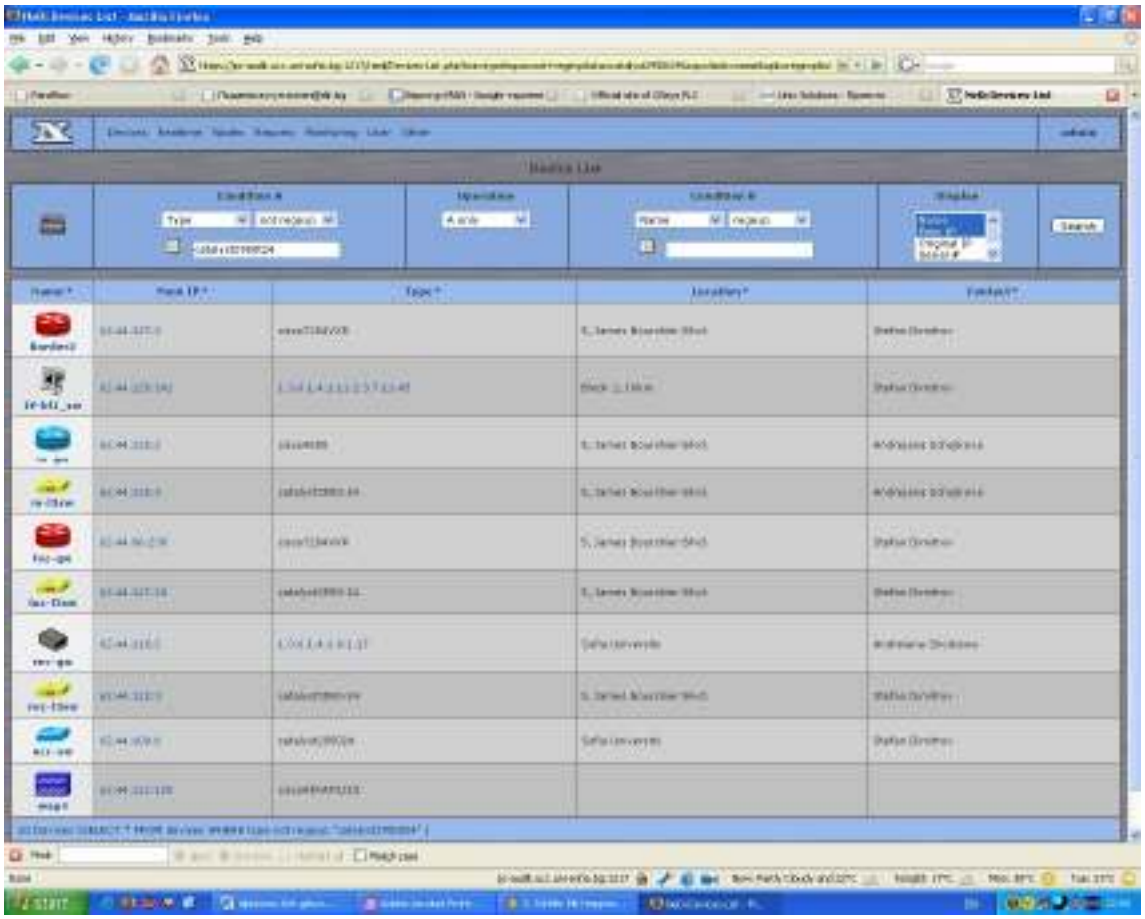
Това са като цяло обектите в мрежата, върху които ще се извърши одита.

Следващата стъпка е извършването на одит тестовете.Те ще се изпълнят с помощта на няколко web базирани приложения:

1. **NeDi** (Network Discovery tool) http://nedi.sourceforge.net

2. **CSA** (Cisco Security Auditor) http://www.cisco.com/en/US/products/ps6263/index.html

На **Фиг. 3.3** са показани данните събрани от NeDi, които ще използваме по-нататък:



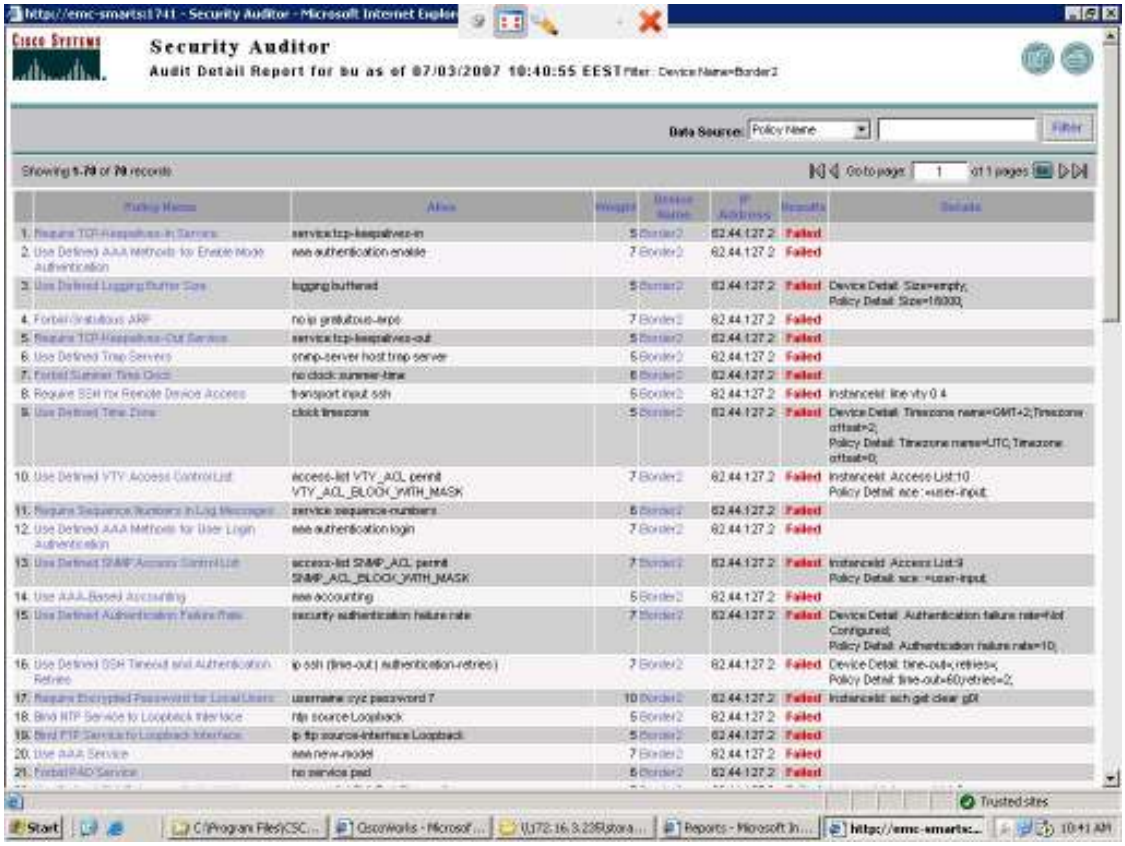
Фиг.3.3. Общ изглед на списъка от устойства,следени от NeDi

Всички събрани данни за мрежовите устройства в мрежата на СУ могат да се разгледат на адрес:
https://pc-audit.ucc.uni-sofia.bg:1217/nedi/ , разбира се,със съответните акаунти за достъп.

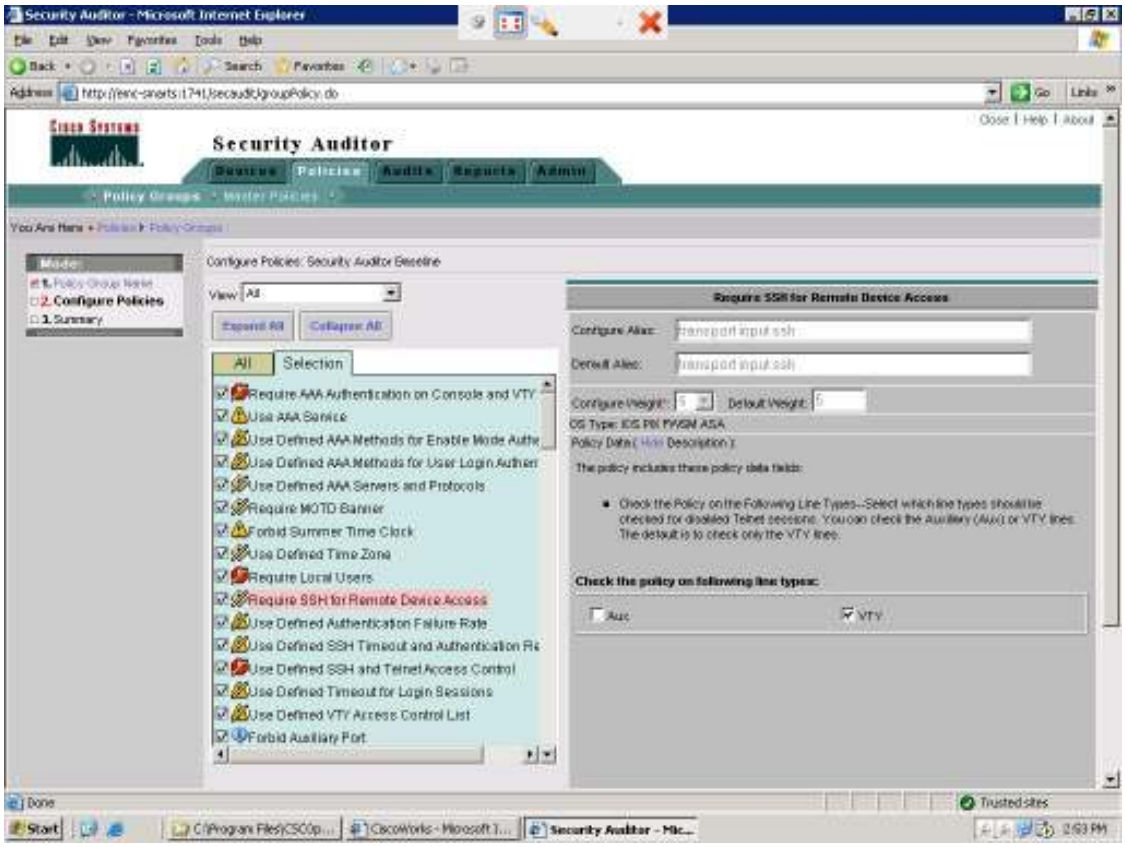
За работата на Cisco Security Auditor не е необходимо да имаме достъп до устройствата от мрежата както и да разполагаме с акаунт за конзолен достъп (telnet/ssh).За тази цел на всяко едно устройство от мрежата добавяме нов потребител с единствено възможни права да гледа конфигурацията.Това става стъпка по стъпка по следният начин:

1) Създаваме privilege level 14, на което единствено разрешаваме изпълнението на командата „sh conf“
2) Създаваме потребител на това ниво на достъп, обвързан със списък за контрол на достъпа (access-list), забраняващ достъп от всички машини с изключение на тази, на която сме инсталирали софтуера за одит.
3) Към съществуващите “access-list-и” на устройствата добавяме адреса на машината, която ще използваме, и я прилагаме на линията за телнет (line vty).
4) Правим друг списък за достъп от snmp сървъра.

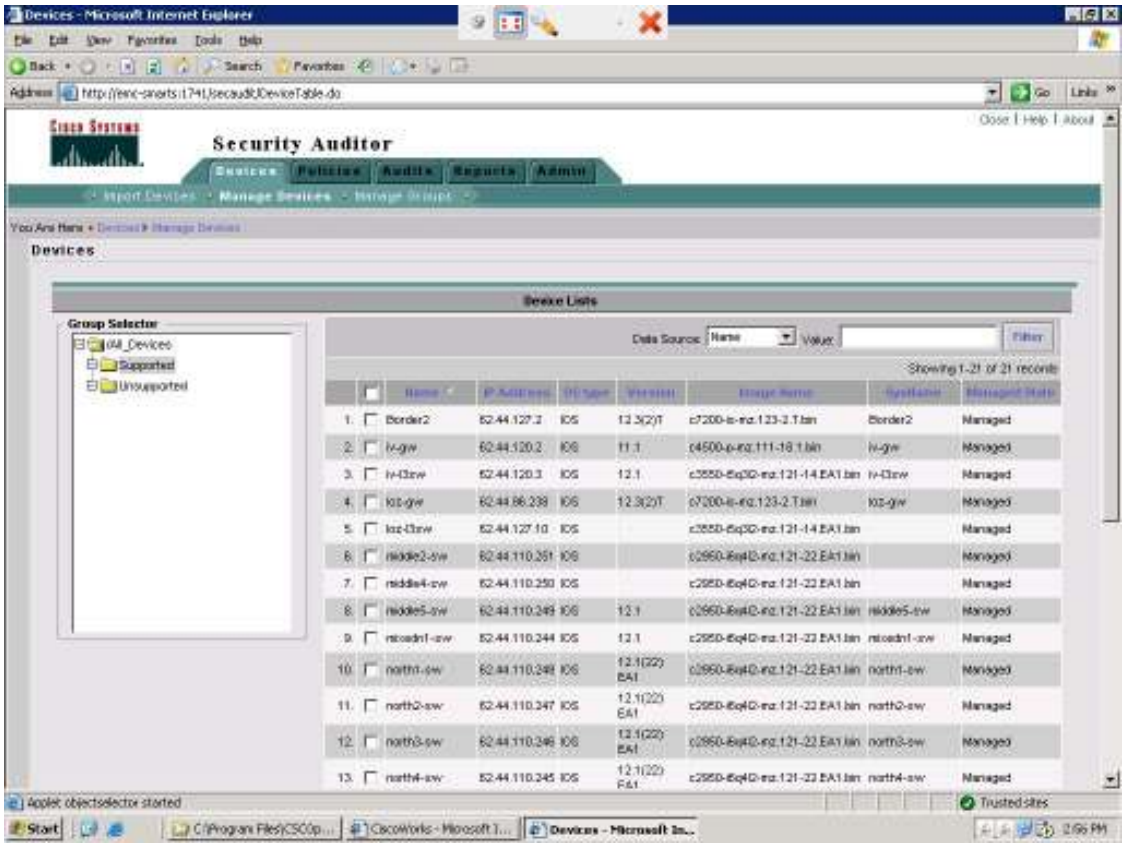
По-долу са дадени няколко екрана (screenshot-a) от Cisco Security Auditor приложението (**Фиг.3.4, Фиг.3.5, Фиг.3.6**):



Фиг.3.4 Отчет за устройството Border2



Фиг.3.5 Списък с правилата, от които са съставени политиките за одит



Фиг.3.6 Списък от устройствата, които ще се анализират.

След като сме въвели данните на всяко едно от устройствана в базите от данни на Nedi и CSA, време е да пуснем да се изпълнява една автоматизирана проверка на сигурността. В нея се включват предефинирани 87 правила, които се смятат за основни изисквания и критерии за сигурност. Разбира се можем да добавим и свои собствени към тях.
Това са правила от вида:

1. Проверка дали е разрешен CDP протокола (Cisco Discovery Protocol) известен със своите уязвимости. (http://nsa2.www.conxion.com/cisco/download.htm)

2. Проверка дали се използва AAA механизма за аутентикация, оторизация и отчетност.
...и много други

Това е резултата от проверката на сигурността на устройството **Border2**. Пълният списък за всички устройства е добавен като Приложение1

Политика	Означение	Устройство	IP адрес	Резултати	Подробности
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOC	Border2	62.44.127.2	Failed	InstanceId: Access List:9 Policy Detail: ace

	K_WITH_MASK				:=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	Border2	62.44.127.2	Failed	
Forbid BOOTP Server	no ip bootp server	Border2	62.44.127.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	Border2	62.44.127.2	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	Border2	62.44.127.2	Failed	
Use Authenticated NTP	ntp authenticate	Border2	62.44.127.2	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	Border2	62.44.127.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	Border2	62.44.127.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	Border2	62.44.127.2	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	Border2	62.44.127.2	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	Border2	62.44.127.2	Failed	
Forbid IP Redirect Message	no ip redirects	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/1.200
Forbid IP Redirect Message	no ip redirects	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.961
Forbid IP Redirect Message	no ip redirects	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.291
Forbid IP Redirect Message	no ip redirects	Border2	62.44.127.2	Failed	InstanceId: FastEthernet0/1.127
Use Defined Authentication Failure Rate	security authentication failure rate	Border2	62.44.127.2	Failed	Device Detail: Authentication failure rate=Not Configured; Policy Detail: Authentication failure rate=10;
Use Defined Timeout for Login Sessions	exec-timeout	Border2	62.44.127.2	Failed	InstanceId: line vty 0 4
Use Defined Timeout for Login Sessions	exec-timeout	Border2	62.44.127.2	Failed	InstanceId: line vty 0 4
Use Defined SSH Timeout and Authentication Retries	ip ssh {time-out | authentication-retries}	Border2	62.44.127.2	Failed	Device Detail: time-out=;retries=; Policy Detail: time-out=60;retries=2;
Require Encrypted Password for Local Users	username xyz password 7	Border2	62.44.127.2	Failed	InstanceId: ach get clear g0l
Forbid Proxy ARP	no ip proxy-arp	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/1.200

Forbid Proxy ARP	no ip proxy-arp	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.961
Forbid Proxy ARP	no ip proxy-arp	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.291
Forbid Proxy ARP	no ip proxy-arp	Border2	62.44.127.2	Failed	InstanceId: FastEthernet0/1.127
Use Defined Severity Level for Console Logging	logging console	Border2	62.44.127.2	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	Border2	62.44.127.2	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	Border2	62.44.127.2	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	Border2	62.44.127.2	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	Border2	62.44.127.2	Failed	
Use Defined Time Zone	clock timezone	Border2	62.44.127.2	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/1.200
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.961
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.291
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	Border2	62.44.127.2	Failed	InstanceId: FastEthernet0/1.127
Use Defined AAA Servers and Protocols	tacacs-server host	Border2	62.44.127.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	Border2	62.44.127.2	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	Border2	62.44.127.2	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	Border2	62.44.127.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	Border2	62.44.127.2	Failed	
Forbid NTP Server service	ntp disable	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/1.200
Forbid NTP Server	ntp disable	Border2	62.44.127.2	Failed	InstanceId:

service					FastEthernet1/0.961
Forbid NTP Server service	ntp disable	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.291
Forbid NTP Server service	ntp disable	Border2	62.44.127.2	Failed	InstanceId: FastEthernet0/1.127
Use Defined TCP Synwait Time	ip tcp synwait-time	Border2	62.44.127.2	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog Servers	logging server	Border2	62.44.127.2	Failed	Device Detail: Log Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Forbid Auxiliary Port	no exec	Border2	62.44.127.2	Failed	
Use AAA Service	aaa new-model	Border2	62.44.127.2	Failed	
Require SSH for Remote Device Access	transport input ssh	Border2	62.44.127.2	Failed	InstanceId: line vty 0 4
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	Border2	62.44.127.2	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	Border2	62.44.127.2	Failed	
Forbid PAD Service	no service pad	Border2	62.44.127.2	Failed	
Use Defined Time Zone	clock timezone	Border2	62.44.127.2	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	Border2	62.44.127.2	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	Border2	62.44.127.2	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	Border2	62.44.127.2	Failed	
Use Defined Logging Buffer Size	logging buffered	Border2	62.44.127.2	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	Border2	62.44.127.2	Failed	InstanceId: line con 0
Use Defined SNMP Community Strings and Access Control	snmp-server community	Border2	62.44.127.2	Failed	Required community string(s) not found Device Detail: ro=Unive***** bio****; Policy Detail: ro=myr***;
Use Defined AAA Methods for Enable Mode	aaa authentication enable	Border2	62.44.127.2	Failed	

Authentication Require Encrypted Line Password	(config-line)#password 7	Border2	62.44.127.2	Failed	InstanceId: line vty 0 4
Use Defined Loopback Interface	interface Loopback	Border2	62.44.127.2	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	Border2	62.44.127.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK _WITH_MASK	Border2	62.44.127.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Minimum Password Length	security passwords min-length	Border2	62.44.127.2	Failed	Device Detail: Min length=Not Configured; Policy Detail: Min length=6;
Forbid IP Unreachable Message	no ip unreachables	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/1.200
Forbid IP Unreachable Message	no ip unreachables	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.961
Forbid IP Unreachable Message	no ip unreachables	Border2	62.44.127.2	Failed	InstanceId: FastEthernet1/0.291
Forbid IP Unreachable Message	no ip unreachables	Border2	62.44.127.2	Failed	InstanceId: FastEthernet0/1.127
Bind Logging Service to Loopback Interface	logging source-interface Loopback	Border2	62.44.127.2	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	Border2	62.44.127.2	Failed	

Border2 устройството е с операционна система Cisco IOS 12.3(2)T , което само по себе си също е предпоставка за известен брой уязвимости, по-важните от които са:

Bug ID	Fixed-in version	Status	Severity ▲
CSCee35379 AAA memory leak after open/close GGSN PPP context	12.2(27)SBA 12.3(8)T1 12.3(9.3)T 12.3(9a)M 12.3(9.3)M 12.2(27)SBB 12.3(7)XM	Fixed	1
CSCed95087 username reset by login command even if login is unsuccessful	12.2(15)BC2e 12.3(7)T1 12.3(7)XL 12.3(8.1)M	Fixed	1

	12.3(8.2)T 12.3(8)T1 12.3(7)XI 12.3(4)T8 12.3(4)XD3		
CSCsb12598 Router forced crash on receiving fragmented TLS ClientHello	12.3(11)JA1 12.2(8)TPC10b 12.2(44.3)S 12.2(42.5)M 12.2(40a)M 12.2(37)SG 12.2(18)SXF8 12.2(15)ZR 12.2(13)ZT 12.1(26)E8 12.1(22)EA10 12.1(22)EA9	Fixed	1
CSCef50650 A 7200 router crashes when it attempt to access a TACACS+ server.	12.3(7)XI2 12.3(7)XI1a 12.3(11.3)T 12.3(11.3)M 12.3(8)YH 12.3(8)YI	Fixed	1
CSCed18557 AS5400 memory leak in Dead Process	12.3(7.2)T 12.3(7.2)M 12.3(7)XI3 12.3(7)XI2 12.3(7)XI1a 12.3(7)T6 12.3(6)M 12.2(27)SBB	Fixed	1
CSCsd85587 7200 Router crashes with ISAKMP Codenomicon test suite	12.2(31)SGA1 12.4(9)T3 12.4(7d)M 12.4(6)XT 12.4(6)T7 12.4(4)XD6 12.4(4)XC6 12.4(9.17)M 12.2(31)SB3c 12.2(25)SEE3 12.2(18.7.15)SXF 12.2(18)ZY 12.2(18)SXF8	Open	1
CSCsd92405 router crashed by repeated SSL connection with malformed finished messag	12.2(31)SB2 12.2(31)SB1b 12.2(29a)SV1 12.2(25)SEE3 12.2(25)S13 12.2(25)EWA9 12.2(18.7.8)SXF 12.2(18)ZY1 12.2(18)SXE6b 12.2(14)S18 12.1(27b)E2	Fixed	1

CSCec25430 IOS may reload from specific packet	12.1(22)EA10 12.1(22)EA9 12.1(19)EA1 12.1(14)AY2 12.1(14)AX2 12.1(13)E14 12.0(5)WC11 12.2(15)XR 12.2(15)T14 12.2(15)MC2a 12.2(15)JK1 12.2(14)SU1 12.2(14)S10 12.2(13)ZH8 12.2(13)T14 12.2(12)DA7 12.3(7)XI 12.3(5b)M 12.3(5.7)T	Fixed	1
CSCee78300 bus error crash (address 0x0) in radius_timers (Router crashes when user tries to authenticate via auth-proxy)	12.2(27)SBA 12.3(14)YQ4 12.3(9b)M 12.3(8)T4 12.4(1a)M 12.4(1.8)T2 12.3(14)YM2 12.2(27)SBB 12.3(10.2)M 12.3(10.2)T 12.3(10)M	Fixed	1
CSCsd44593 On error, auto-generated SSL cert is regenerated with same serial number	12.4(7.17)T 12.4(7.17)M 12.3(18.8)M	Fixed	3 Workaround Exists

Списък от откритите проблеми по текущите софтуерни версии (IOS) на останалите устройства ще добавя също към приложение 2.

Глава IV. Оценка,анализ и препоръки за бъдещото развитие

Анализът на резултатите от одита можем да започнем с факта, че политика за сигурност в мрежата на СУ не съществува, нито процедури или някакви насоки по запазването на сигурността (засега поне, може това да е тема на бъдеща дипломна работа)

Това автоматично дава отговора и на няколко други въпроси:
1.Няма писмено установени правила за това кое е разрешено и кое не е;
2.Преди да се дадат права за достъп, на потребителите и персонала не е обяснено какви са задълженията им във връзка със опазването на сигурността;
3.Не се прави преглед, коментар и обновяване на тези политики за сигурност през определен интервал от време;
4.Няма писмени процедури за това как се извършва оторизацията, на кого и как се дават права за работа с определени системи/ мрежови устройства /достъп до мрежата, а също така и как се прекратява достъпа на бивши служители и потребители;
5.Няма ясно определено условие Интернет доставчикът да защитава преминаващият от и към него него трафик на СУ.

След като установихме липсата на тези основни изисквания, можем да направим оценка на мрежовата сигурност отдолу нагоре по слоевете от OSI модела.

4.1 Физическа защита

Както споменах по-горе, няма процедури за физически достъп до устройствата в мрежата. Дали до тях да има отдалечен достъп, дали той да е денонощен или само в рамките на работния ден или по някаква друга часова схема, кой да има възможност да го прави, кой да реагира при евентуален инцидент, при който се налага физически да се достигне до устройството. Така наречената чувствителна зона, където се намират мрежовите устройства например е стаята, в която се помещава и персонала на Изчислителният Център в момента. (По принцип устройствата имат различни изисквания за температура и влажност от хората и е препоръчително да са отделени.) Достъп до стаята имат персонала на УИЦ. За да се влезе, е нужно да се изключи съответната аларма, което се прави от охраната. Това само по себе си е много добре, като се изключи факта, че липсват устройства за денонощно наблюдение (например камери), както и датчици за пожар, температура, влажност и др.
Другото, което би било полезно, е мрежовите администратори да носят някакъв отличителен знак, карта, за да може охраната да ги идентифицира.

4.2 Защита на слой 2 от OSI модела

Към нея можем да отнесем първо защитата от това неоторизирани крайни устройства (работни и мобилни станции) да се свързват към мрежата и да извършат многобройни атаки (виж **глава 2**). Това може да стане, като се конфигурират опции за сигурност (port security) на портовете на крайните мрежови устройства (комутатори), което обаче не е направено. Трябва да имаме предвид, че компрометирането на

мрежата на този слой автоматично означава, че и горните слоеве вече са изложени на риск.
Можем да кажем, че някои от основните изисквания за сигурността, така наречените „добри практики за сигурност" (security best practises) не са спазени на този слой:
1. Неизползваните портове не се спират и не се конфигурират в VLAN, който не се използва.
Някои от тези изисквания са налице:
2. VLAN 1 не се използва за нищо и се спира;

3. Уговарянето на trunk се забранява. DTP протоколът се спира с изключение на устройствата rec-l3sw, loz-l3sw, iv-l3sw. Това са устройствата за връзка към MAN мрежата на София Комюникейшънс, най-вероятно това е тяхно изискване.

4. Изрично се конфигурира trunking на нужните връзки.

5. Използва се 802.1q таг на всички trunk връзки.
--мерките споменати до тук се правят с цел предотвратяване на атаката VLAN Hopping

6. Липсва обаче конфигурацията на port security на интерфейсите и определяне броят на машините (съответно MAC адресите), които могат да се научават на даден порт на комутатора и действието, което да се предприеме, когато тази бройка бъде достигната. За препоръчване е изключване на порта - shutdown. Конфигурирането на този детайл може да предпази мрежата на СУ от атака върху CAM таблицата и т.нар. атака „изяждане на DHCP ресурси".

7. Не точно към този слой, но в контекста на написаното тук, можем да отнесем липсата на мониторинг система, която да уведомява за проблеми в реално време: при проблем да изпраща на администраторите съобщение по електронна поща или sms. (Знаем вече,че при повечето DoS атаки ресурсите на комутаторите, най-вече процесора (CPU), се заемат на почти 100%. Така че едно съобщение, алармиращо за много висок процент на използване на CPU-то, може да говори за евентуално наличие на такава атака.)

8. Липсва конфигурация на „DHCP snooping":
По подразбиране DHCP пакети могат да се получават на всеки порт на комутатора. За да става това само на портовете, към които са закачени DHCP сървъри, комутаторите трябва да се конфигурират по следния начин:

Interface Commands
ip dhcp snooping trust
Global Commands
ip dhcp snooping vlan 4,104
offer, ack, nak
no ip dhcp snooping information option
ip dhcp snooping

9. Силно препоръчително е да се направи статично обвързване (binding) на интерфейс с MAC адрес на машината, която се включва към него. Така се избягват ARP атаки, прихващане на ARP заявки и отговори:

Switch#conf t
Switch(config)#ip source binding 0000.0000.0001 vlan 4 10.0.10.200 interface fastethernet 3/1

Също така е препоръчително да за направи статичен ARP запис за важните рутери и хостове:
Switch(config)# arp interface_name ip_address mac_address

10. Много важен пропуск е липсата на конфигурирани bpduguard и root guard функционалности на интерфейсите: те предпазват мрежата от това неоторизиран комутатор да бъде закачен на някой порт от мрежата и да стане корен на „разпереното дърво" (Spanning-tree), като по този начин промени по непредсказуем начин логическата топология на цялата мрежа.

11. Като положително тук може да отбележим забраняването на CDP (Cisco Discovery Protocol). Чрез него евентуален нападател би получил информация за устройствата в мрежата, тяхното разположение и конфигурация.

12. По-скоро като препоръка за улеснение, а не от гледна точка на сигурността препоръчително е да се конфигурира VTP протокола с MD5 аутентикация с цел повишаване на сигурността. (Има настроен VTP само на su-backbone-sw устройството, което само по себе си е безсмислено)

4.3 Защита на L3 от OSI модела

Първото нещо, което искам да посоча тук, е факта, че СУ разполага с адресно пространство 62.44.96.0 – 62.44.127.255, което е доста много. Това обаче не означава, че е добра практика обикновените работни и мобилни станции в мрежата на СУ да са с публични адреси. Препоръката ми е поне за тях да се използва NAT функциалността, а публични IP адреси да се заделят само за сървърите за различните услуги, които се достъпват отвън.
Другите препоръки за L3 можем да видим директно в отчета на софтуера на Сиско:

На различните устройства:
no ip source-route --global
deny ip RFC2827 --interface
no ip gratuitous-arps --global
no ip redirects --на routed interface
no ip proxy-arp --на routed interface
ip tcp synwait-time --global
no ip unreachables –global & L3 interface mode
...и още,пълният списък може да се види в Приложение 1

4.3 Защита на L4-L7

Управление на комутатора:
Всички тези защити, които бяха описани по-горе, няма да струват нищо, ако евентуално нападателят може да осъществи телнет сесия към устройството и ги забрани. Точно затова наблюдението и управлението на комутатора би се превърнало в една от най-големите му слабости. Повечето от протоколите за

управление са несигурни (syslog, SNMP, TFTP, Telnet, FTP и т.н). А е така, защото информацията се предава в „открит текст” - некриптиран вид. Това означава, че ако някой злодеятел се върже към мрежата и „подслуша” трафика, ще може лесно да улови паролите за достъп. За препоръчване е да се използват сигурните им варианти (SSH, SCP, SSL, OTP и т.н), а където е възможно - и *Out- of-Band (OOB) management* (менажирането на устройствата да се извършва по отделен от публичния канал (интерфейс или платка), независещ от това дали устройството е работещо в момента и дали е достъпно по нормалния начин.)
Другото изискване, което бих добавила, е машините, които извършват наблюдението, да бъдат в отделен VLAN - management VLAN, различен от стандартните потребителски, където да не минава нищо друго освен трафик, свързан с управлението и наблюдението на устройствата.

За съжаление само на 3 от устройствата в мрежата на СУ има пусната SSH услуга. Нужно е след пускането на й в действие по комутаторите да се разреши логването към устройството единствено и само по този протокол:
```
Switch(config)#line vty 0 15
Switch(config-line)#transport input ssh
```

Като се има предвид, че не се ползва, препоръчително е услугата „http server” на устройството su-backbone-sw да се спре: (пусната е само на него, най-вероятно е останало от предишен тест)
```
su-backbone-sw(config)# no ip http server
```

Похвален е стремежа на всички устройства да се конфигурират списъци за достъп само от 2 определени машини ady.uni-sofia.bg (62.44.96.7) и ns.uni-sofia.bg (62.44.96.1), свързването към които става по ssh протокола. За съжаление „пътят” от тези 2 машини до някои от устройствата минава отново през MAN мрежата на „София Комюникейшънс”. По този път паролите на telnet протокола преминават в „чист вид”, което далеч не ни гарантира сигурност.

По мое мнение силно наложително е в мрежата да се пусне RADIUS сървър, който да предлага както AAA услугите – Authentication, Authorization, Accounting, така и да събира системните логове на устройствата. Това е почти задължително като се има предвид, че повече от един човек има достъп до устройствата. Нужно е всеки от персонала да е с различен акаунт, което би спомогнало за по-добра отчетност.
А това много трудно би станало без централизиран сървър, на който да се създават и мениджират тези акаунти, и, към който да се свързват устройствата, когато има нужда от аутентикация. Конфигурацията може да стане евентуално по следния начин:

```
aaa new-model
aaa authentication login default group radius local
aaa authentication enable default group radius none
aaa authorization exec default group radius none
aaa authorization commands 15 default group radius none
aaa accounting commands 15 default start-stop group radius
```

4.4 Препоръки за самите устройства

Както вече много пъти споменах, операционната система на устройствата е от голямо значение за сигурността на цялата мрежова инфраструктура. От версията на Cisco IOS зависи както възможностите и услугите, които мрежовото устройство предлага, така и сигурността ни. Колкото по-стара е операционната система по принцип, толкова повече открити уязвимости и проблеми има в нея. Затова е важно винаги да се използва последната излязла стабилна такава, на която да са приложени съответните „кръпки" по сигурността (security patches). За съжаление, като цяло в мрежата на СУ операционните системи на Сиско устройствата не се обновяват периодически. Извадка за това какви уязвимости са открити досега в текущите версии на IOS-те в СУ , както и списък на версиите, в които се разрешава дадената уязвимост, може да намерите в Приложение 1.
Прилагам списък с препоръчителните версии на операционните системи на устройствата, към които трябва да се премине:

Border2,loz-gw:
current boot image: `c7200-is-mz.123-2.T.bin`

Platform:	7200			
File name		**Min. Memory (MB)**	**Min. Flash (MB)**	**Date Released**
c7200-is-mz.123-14.T7.bin		128	48	27-MAR-2006

su-backbone-sw, ucc-sw, swi-008:
current boot image: `c2950-i6k2l2q4-mz.121-22.EA7.bin`

Platform:	CAT2950
Release:	12.1.22-EA10 (ED - Early Deployment)
Software Feature Sets:	C2950 EI AND SI IOS IMAGE AND WEB BASED DEVICE MANAGER

всички останали комутатори Catalyst 2950: (`middle2-sw`, `middle4-sw`, `middle5-sw`, `mixedn1-sw`, `north1-sw`, `north2-sw`, `north3-sw`, `north4-sw`, `rector-sw`, `south2-sw`, `south3-sw`, `south4-sw`)
current boot image: `c2950-i6q4l2-mz.121-22.EA1.bin`

Platform:	CAT2950
Release:	12.1(22)EA1b (ED - Early Deployment)
Software Feature Sets:	C2950 EI AND SI IOS IMAGE AND WEB BASED DEVICE MANAGER

rec-l3sw, iv-l3sw и loz-l3sw:
current boot image: `c3550-i5q3l2-mz.121-14.EA1.bin`

Platform:	CAT3550
Release:	12.1.22-EA10 (ED - Early Deployment)
Software Feature Sets:	C3550 EMI IOS IMAGE AND WEB BASED DEVICE MANAGER

iv-gw:
current boot image: `c4500-p-mz.111-18.1.bin`

Platform:	4500		
Release:	12.1.27b (GD - General Deployment)		
Software Feature Sets:	SERVICE PROVIDER		
c4500-p-mz.121-27b.bin	32	8	24-AUG-2005

rec-gw:
current boot image: `c2500-i-l.120-14.bin` Това е версия от 2000 година. Софтуерът, с който работихме, също не можа да разпознае устройството заради старата версия на операционната система. Това устройство се класифицира от Сиско в период End-of-Sales, което означава,че в момента вече не се продава, а скоро няма и да се поддържа – затова тук препоръката е по-скоро самото то да се замени, отколкото да се подновява софтуера му.

Platform:	2501-2525		
Release:	12.0.28d (GD - General Deployment)		
Software Feature Sets:	IP		
c2500-i-l.120-28d.bin	6	8	25-AUG-2005

4.5 Общи препоръки

1. Ще започна с това винаги да се използва лицензиран софтуер, било той платен или под GPL лиценз!
Това важи едновременно и за мрежовите устройства, и за крайните работни станции и сървери, които извършват управлението и наблюдението над тях. Използвайки го, сме сигурни, че няма да донесем в мрежата вируси, троянски коне или всякакъв друг вид зловреден код.

2. С най-голям приоритет според мен, освен политиката за сигурност, е създаването на пълна и актуална документация, която да включва:
- Логическата топология на мрежата – как са свързани устройствата, в кой PoP са разположени и какви сегменти има зад тях; (почти пълна такава може да се види на **Фиг 3.2** от 3-та Глава)
- Физическата топология на мрежата – кои точно интерфейси се използват за връзка между устройствата, какъв е типа на модулите за свързване между тях (GBIC/SFP,SX/LX/ZX), какъв е типа и вида на кабелите (Fibre Optic,Single/Multi Mode,LC/SC). В момента съществува единствена схема, която е нещо средно между двете, но по-лошото е, че е доста неактуална.
- Информация за VLAN-те – кой до къде се разпростира, какви потребители се включват в него, кои портове са в него на различните комутатори и каква е адресната схема в него на трети слой. (В момента съществува непълен списък, който описва единствено VLAN-те, които минават през MAN-а на „София Комюникейшънс”.)
- Документ със списъци от устройствата, хардуерната им платформа, версиите на операционната система (ОС), както и кога са правени промени по тях – хардуерни или софтуерни – обновявания на ОС, прилагане на различни кръпки (patch) по него, добавяне и подмяна на модули, платки, интерфейси. (Това вече може да се види чрез приложението **NeDi**, което инсталирахме, за да ни помогне да извършим одита.)

- Документ с особенностите на мрежовата конфигурация – къде има някаква специфика и на кои части от конфигурациите трябва да се обърне особенно внимание при нужда от бързо разрешаване на възникнали проблеми (troubleshouting).
- Документ как е разделено IP адресното пространство на СУ по възли (PoPs), как са раздадени IP адресите, кой на коя работна станция е зададен, колко и кои от тях са статични и кои се раздават по DHCP.
- Списък с услугите, които се предлагат в различните PoPs. (В общият случай това означава дали навсякъде се разпространяват дадените VLAN-и), дали във всички тях се предлагат LAN достъп, достъп до Интернет, мениджмънт на мрежовите устройства, работа на IP телефони и т.н
- Документ кои потребители и системи до кои съответно трябва да имат достъп. (Т.е ясно описание и обосновка на текущите списъци за контрол на достъпа и конфигурирания рутинг между мрежите.)
- План за евентуални бъдещи промени по мрежата – подмяна на устройства, модули, обновяване на операционни системи, включващ точното време и процедура, по които ще се извърши и влиянието, което ще има върху системите и потребителите, както и списък от тестовете, които ще се извършат след това за проверка дали планираната промяна е била успешна.

3. Да се направи ясна процедура по архивиране и възстановяване на данните (backup и restore). В момента за архивиране на конфигурациите на мрежовите устройства се използва системата Trac : (https://62.44.109.56:1217/trac/netdiv). За съжаление архивирането се прави само ръчно, без да има определен период от време, през който да се извършва, или без да има система, която да следи за промяна по конфигурацията и да изтегля новата автоматично. Липсва и система за архивиране на системните логове от устройствата, което би било доста важно, ако при евентуални атаки по мрежата искаме да открием причината за тях и източникът им. Другото нещо, за което трябва да се помисли, е периодичното архивиране на данните от машината с адрес 62.44.109.56. За да се запазят, ако евентуално се случи някакакъв проблем с нея. Разбира се, трябва да се има предвид и запазването на сигурността на архивираните данни. (Ако злодеятел има достъп до тях, това ще означава и че има достъп до конфугурацията и логовете на цялата мрежа.)

4. Да се организират различни видове обучения, семинари и курсове за подобряване квалификацията на персонала, за да сме сигурни, че те могат и ще могат да работят и поддържат адекватно системите и мрежовата инфраструктура на СУ. Също така да се провежда и кратко обучение на потребителите вътре в мрежата за това как да работят в нея и как да полагат усилия за запазването на сигурността й.
Това може да стане също и онлайн. В момента за портал и място където се държи полезна документация служи сайта http://ucc.uni-sofia.bg/ .

5. Тъй като в момента защитата от вируси, всякакъв друг зловреден код, както и външни DoS, фрагментирани или с преправени пакети атаки е изнесена на външна машина (Border 1), която има маршрутизиращи функции, но не е специализирано мрежово устройсто, бих препоръчала евентуалното използване на хардуерна защитна стена на входа на мрежата на СУ - например *Cisco PIX 515E Security Appliance* или по-новото комбинирано решение на Сиско - *Cisco ASA 5500 Series Adaptive Security Appliances*. Което, разбира се, зависи и от бюджета, който е отделен за сигурност в мрежата.

4.6 Обобщение и крайна оценка

Като цяло мога да кажа, че в мрежата на СУ има голям стремеж за запазването на сигурността, както и разбира се, трябва и да бъде. Повечето от изискванията за така наречените „security best practices” са спазени ,без изключенията за които съм споменала по-горе. Основната насока, в която трябва да се работи, е най-вече създаването на политика за сигурност и реализирането й. Също така документиране на текущото състояние на мрежата, промените, които се правят по нея и проблемите по сигурността, възникаващи от това.
Другото нещо, което като цяло трябва да се промени, е стремеж към по-често обновяване на операционните системи на мрежовите устройства и изобщо въвеждане на повече нови технологии и услуги в мрежата на СУ. (За съжаление това може би също зависи от бюджета, отпуснат за поддръжка и развитие на мрежата и запазване на сигурността в нея.)

Заключение

След като сега вече знаем как се пише политика за сигурност, е време да се направи такава и за мрежата на Софийският университет.В нея могат да бъдат включени както резултатите от одита и преоръките от настоящата дипломна работа, така и множеството правила и проблемни моменти, които със сигурност съм пропуснала. Важно е да запомним, че една политика за сигурност и изобщо всички правила по сигурността не са нещо фиксирано, те трябва периодически да се преразглеждат, допълват и обновяват, за да са готови да посрещат новите предизвикателства пред сигурността.

В заключение отново ще изтъкна факта, че главната цел на мрежовия специалист е да повиши устойчивостта на мрежата, невъзможно е тя да е защитена на сто процента. Винаги съществува човешкия фактор за грешка, както и бъгове в софтуера и хардуерни дефекти.

Целта на всеки един специалист по сигурността е да направи така, че системата винаги да е защитена на ниво с една крачка по напред от възможностите на хората които искат да проникват в нея.

Използвана литература:

1. Government of the Hong Kong Special Administrative Region**,Security Risk Assessment & Audit Guidelines**

2. Jazib Frahim, **Cisco Press Cisco ASA All-in-One Firewall IPS and VPN Adaptive Security Appliance**

3. Dave Hucaby, **Cisco ASA and PIX Firewall Handbook**

4. Duane De Capite, **Self-Defending Networks: The next generation of network security**

5. Andrew Whitaker, **Penetration Testing and Network Defense**

6. **Cisco Certified Network Professional curriculum**

7. **Cisco Certified Network Security curriculum**

8. Gert De Laet**, Network Security Fundamentals**

9. **Cisco** Connection Online (**CCO**) http://cco.cisco.com

10. NSA Router Security Configuration Guide: http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1

11. http://www.cisco.com/warp/public/778/security/vuln_stats_02-03-00.html

12. http://www.cisco.com/web/learning/le31/le29/configuring_asa_pix_security_appliances.html

Приложение 1

Данни за устройство: **loz-gw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	loz-gw	62.44.96.238	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	loz-gw	62.44.96.238	Failed	
Forbid BOOTP Server	no ip bootp server	loz-gw	62.44.96.238	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-gw	62.44.96.238	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	loz-gw	62.44.96.238	Failed	
Use Authenticated NTP	ntp authenticate	loz-gw	62.44.96.238	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	loz-gw	62.44.96.238	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	loz-gw	62.44.96.238	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	loz-gw	62.44.96.238	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	loz-gw	62.44.96.238	Failed	
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/3 Policy Detail: ace =user-input;
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/2 Policy Detail: ace =user-input;
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/1 Policy Detail: ace =user-input;
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.232 Policy Detail: ace =user-input;
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.3 Policy Detail: ace =user-input;
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.1 Policy Detail: ace =user-input;

Forbid IP Redirect Message	no ip redirects	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/1
Forbid IP Redirect Message	no ip redirects	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/1.161
Forbid IP Redirect Message	no ip redirects	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.232
Forbid IP Redirect Message	no ip redirects	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.130
Use Defined Authentication Failure Rate	security authentication failure rate	loz-gw	62.44.96.238	Failed	Device Detail: Authentication failure rate=Not Configured; Policy Detail: Authentication failure rate=10;
Use Defined SSH Timeout and Authentication Retries	ip ssh {time-out | authentication-retries}	loz-gw	62.44.96.238	Failed	Device Detail: time-out=;retries=; Policy Detail: time-out=60;retries=2;
Require Encrypted Password for Local Users	username xyz password 7	loz-gw	62.44.96.238	Failed	InstanceId: ach get clear arp g0l
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/1
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/1.161
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.232
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	loz-gw	62.44.96.238	Failed	
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.130
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.4
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.3
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.2
Forbid Proxy ARP	no ip proxy-arp	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.1
Require MOTD Banner	banner motd	loz-gw	62.44.96.238	Failed	
Use Defined Severity Level for Console Logging	logging console	loz-gw	62.44.96.238	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	loz-gw	62.44.96.238	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	loz-gw	62.44.96.238	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	loz-gw	62.44.96.238	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	loz-gw	62.44.96.238	Failed	
Use Defined Time Zone	clock timezone	loz-gw	62.44.96.238	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;

Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/1
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/1.161
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.232
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.130
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.4
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.3
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.2
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.1
Use Defined AAA Servers and Protocols	tacacs-server host	loz-gw	62.44.96.238	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-gw	62.44.96.238	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	loz-gw	62.44.96.238	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	loz-gw	62.44.96.238	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-gw	62.44.96.238	Failed	
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: Serial2/1
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/1.161
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.232
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.130
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.4
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.3
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.2
Forbid NTP Server service	ntp disable	loz-gw	62.44.96.238	Failed	InstanceId: FastEthernet0/0.1
Use Defined TCP Synwait Time	ip tcp synwait-time	loz-gw	62.44.96.238	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog	logging server	loz-gw	62.44.96.238	Failed	Device Detail: Log

Servers			8		Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Forbid Auxiliary Port	no exec	loz-gw	62.44.96.23 8	Failed	
Use AAA Service	aaa new-model	loz-gw	62.44.96.23 8	Failed	
Require SSH for Remote Device Access	transport input ssh	loz-gw	62.44.96.23 8	Failed	InstanceId: line vty 0 4
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	loz-gw	62.44.96.23 8	Failed	InstanceId: FastEthernet0/0.4 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	loz-gw	62.44.96.23 8	Failed	InstanceId: FastEthernet0/0.3 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	loz-gw	62.44.96.23 8	Failed	InstanceId: FastEthernet0/0.1 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	loz-gw	62.44.96.23 8	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	loz-gw	62.44.96.23 8	Failed	
Forbid PAD Service	no service pad	loz-gw	62.44.96.23 8	Failed	
Use Defined Time Zone	clock timezone	loz-gw	62.44.96.23 8	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	loz-gw	62.44.96.23 8	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	loz-gw	62.44.96.23 8	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	loz-gw	62.44.96.23 8	Failed	
Use Defined AAA	aaa authentication	loz-gw	62.44.96.23	Failed	

Methods for Enable Mode Authentication	enable		8		
Use Defined			62.44.96.23		Device Detail: Size=empty;
Logging Buffer Size	logging buffered	loz-gw	8	Failed	Policy Detail: Size=16000;
Require Encrypted	(config-		62.44.96.23		
Line Password	line)#password 7	loz-gw	8	Failed	InstanceId: line vty 0 4
Require Encrypted	(config-		62.44.96.23		
Line Password	line)#password 7	loz-gw	8	Failed	InstanceId: line con 0
					Required community string(s) not found
Use Defined SNMP					Device Detail: ro=EXTt****
Community Strings	snmp-server		62.44.96.23		bio****;
and Access Control	community	loz-gw	8	Failed	Policy Detail: ro=myr***;
Use Defined			62.44.96.23		Loopback interface
Loopback Interface	interface Loopback	loz-gw	8	Failed	mismatched or missed.
Forbid IP Unreachable Messages for Null			62.44.96.23		
Interface	no ip unreachables	loz-gw	8	Failed	
	access-list VTY_ACL permit				InstanceId: Access List:10
Use Defined VTY	VTY_ACL_BLOCK_		62.44.96.23		Policy Detail: ace :=user-
Access Control List	WITH_MASK	loz-gw	8	Failed	input;
Use Defined					Device Detail: Min
Minimum Password	security passwords		62.44.96.23		length=Not Configured;
Length	min-length	loz-gw	8	Failed	Policy Detail: Min length=6;
Forbid IP Unreachable			62.44.96.23		
Message	no ip unreachables	loz-gw	8	Failed	InstanceId: Serial2/1
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/1.161
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.232
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.130
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.4
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.3
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.2
Forbid IP Unreachable			62.44.96.23		InstanceId:
Message	no ip unreachables	loz-gw	8	Failed	FastEthernet0/0.1
Bind Logging Service to Loopback	logging source-		62.44.96.23		
Interface	interface Loopback	loz-gw	8	Failed	
Require TCP-Keepalives-Out	service tcp-		62.44.96.23		
Service	keepalives-out	loz-gw	8	Failed	

Данни за устройство: **loz- l3sw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Cisco Express Forwarding	ip cef	loz-l3sw	62.44.127.10	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	loz-l3sw	62.44.127.10	Failed	
Use Defined Logging Buffer Size	logging buffered	loz-l3sw	62.44.127.10	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Use Time Stamps for Debugging Messages	service timestamps debug	loz-l3sw	62.44.127.10	Failed	
Forbid Gratuitous ARP	no ip gratuitous-arps	loz-l3sw	62.44.127.10	Failed	
Forbid HTTP Service	no ip http server	loz-l3sw	62.44.127.10	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	loz-l3sw	62.44.127.10	Failed	
Require MOTD Banner	banner motd	loz-l3sw	62.44.127.10	Failed	
Use Defined Trap Servers	snmp-server host trap server	loz-l3sw	62.44.127.10	Failed	
Require Local Users	username xyz password 7	loz-l3sw	62.44.127.10	Failed	InstanceId: No Local user specified
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	loz-l3sw	62.44.127.10	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Require Sequence Numbers in Log Messages	service sequence-numbers	loz-l3sw	62.44.127.10	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-l3sw	62.44.127.10	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	loz-l3sw	62.44.127.10	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Require Local Users	username xyz password 7	loz-l3sw	62.44.127.10	Failed	InstanceId: No Local user specified
Use AAA-Based Accounting	aaa accounting	loz-l3sw	62.44.127.10	Failed	
Forbid CDP	no cdp run	loz-l3sw	62.44.127.10	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	loz-l3sw	62.44.127.10	Failed	
Use Defined NTP Server	ntp server	loz-l3sw	62.44.127.10	Failed	Device Detail: NTP Servers=; Policy Detail: NTP Servers=;
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	loz-l3sw	62.44.127.10	Failed	
Use AAA Service	aaa new-model	loz-l3sw	62.44.127.10	Failed	
Forbid PAD Service	no service pad	loz-l3sw	62.44.127.10	Failed	
Require Enable	enable password	loz-l3sw	62.44.127.10	Failed	

Password					
	access-list SNMP_ACL permit				InstanceId: Access List:9
Use Defined SNMP Access Control List	SNMP_ACL_BLOCK_WITH_MASK	loz-l3sw	62.44.127.10	Failed	Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	loz-l3sw	62.44.127.10	Failed	Device Detail: Severity=disable; Policy Detail: Severity=emergencies;
Forbid BOOTP Server	no ip bootp server	loz-l3sw	62.44.127.10	Failed	
Use Defined Severity Level for Console Logging	logging console	loz-l3sw	62.44.127.10	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined AAA Servers and Protocols	tacacs-server host	loz-l3sw	62.44.127.10	Failed	
Forbid IP Source Routing	no ip source-route	loz-l3sw	62.44.127.10	Failed	
Use Defined SNMP Community Strings and Access Control	snmp-server community	loz-l3sw	62.44.127.10	Failed	Required community string(s) not found Device Detail: ro=; Policy Detail: ro=myr***;
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-l3sw	62.44.127.10	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	loz-l3sw	62.44.127.10	Failed	
Use Time Stamps for Logging	service timestamps log	loz-l3sw	62.44.127.10	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	loz-l3sw	62.44.127.10	Failed	
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	loz-l3sw	62.44.127.10	Failed	
Use Defined TCP Synwait Time	ip tcp synwait-time	loz-l3sw	62.44.127.10	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	loz-l3sw	62.44.127.10	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	loz-l3sw	62.44.127.10	Failed	
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	loz-l3sw	62.44.127.10	Failed	InstanceId: CEF not enabled in device
Use Defined Loopback Interface	interface Loopback	loz-l3sw	62.44.127.10	Failed	Loopback interface mismatched or missed.
Require Password Encryption Service	service password-encryption	loz-l3sw	62.44.127.10	Failed	
Use Defined Syslog Servers	logging server	loz-l3sw	62.44.127.10	Failed	Device Detail: Log Servers=Not defined;

					Policy Detail: Log Servers=Any is ok;
Bind Logging Service to Loopback Interface	logging source-interface Loopback	loz-l3sw	62.44.127.10	Failed	
	access-list VTY_ACL permit				InstanceId: Access List:10
Use Defined VTY Access Control List	VTY_ACL_BLOCK_WITH_MASK	loz-l3sw	62.44.127.10	Failed	Policy Detail: ace :=user-input;
Use Authenticated NTP	ntp authenticate	loz-l3sw	62.44.127.10	Failed	The device is not configured with NTP authentication.
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	loz-l3sw	62.44.127.10	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	loz-l3sw	62.44.127.10	Failed	

Данни за устройство: **swi_008**

Policy Name	Alias	Device Name	IP Address	Results	Details
	access-list SNMP_ACL permit				InstanceId: Access List:9
Use Defined SNMP Access Control List	SNMP_ACL_BLOCK_WITH_MASK	swi_008	62.44.96.19	Failed	Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	swi_008	62.44.96.19	Failed	
Forbid BOOTP Server	no ip bootp server	swi_008	62.44.96.19	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	swi_008	62.44.96.19	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	swi_008	62.44.96.19	Failed	
Use Authenticated NTP	ntp authenticate	swi_008	62.44.96.19	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	swi_008	62.44.96.19	Failed	
	access-list VTY_ACL permit				InstanceId: Access List:10
Use Defined VTY Access Control List	VTY_ACL_BLOCK_WITH_MASK	swi_008	62.44.96.19	Failed	Policy Detail: ace :=user-input; Device Detail: Severity=debugging;
Use Defined Severity Level for Console Logging	logging console	swi_008	62.44.96.19	Failed	Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	swi_008	62.44.96.19	Failed	
Require Password	service password-	swi_008	62.44.96.19	Failed	

Encryption Service	encryption				
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	swi_008	62.44.96.19	Failed	
Forbid IP Redirect Message	no ip redirects	swi_008	62.44.96.19	Failed	InstanceId: Vlan3
Use Defined Logging Buffer Size	logging buffered	swi_008	62.44.96.19	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Require Encrypted Password for Local Users	username xyz password 7	swi_008	62.44.96.19	Failed	InstanceId: ach g0l
Forbid Proxy ARP	no ip proxy-arp	swi_008	62.44.96.19	Failed	InstanceId: Vlan3
Require MOTD Banner	banner motd	swi_008	62.44.96.19	Failed	
Use Defined Severity Level for Console Logging	logging console	swi_008	62.44.96.19	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	swi_008	62.44.96.19	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	swi_008	62.44.96.19	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	swi_008	62.44.96.19	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	swi_008	62.44.96.19	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	swi_008	62.44.96.19	Failed	
Use Defined Time Zone	clock timezone	swi_008	62.44.96.19	Failed	Device Detail: Timezone name=GMT+2;Time zone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	swi_008	62.44.96.19	Failed	InstanceId: Vlan3
Use Defined AAA Servers and Protocols	tacacs-server host	swi_008	62.44.96.19	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	swi_008	62.44.96.19	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	swi_008	62.44.96.19	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	swi_008	62.44.96.19	Failed	
Use Defined AAA Methods for User	aaa authentication login	swi_008	62.44.96.19	Failed	

Login Authentication					
Forbid NTP Server service	ntp disable	swi_008	62.44.96.19	Failed	InstanceId: Vlan3
Use Defined TCP Synwait Time	ip tcp synwait-time	swi_008	62.44.96.19	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog Servers	logging server	swi_008	62.44.96.19	Failed	Device Detail: Log Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Use AAA Service	aaa new-model	swi_008	62.44.96.19	Failed	
Require SSH for Remote Device Access	transport input ssh	swi_008	62.44.96.19	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	swi_008	62.44.96.19	Failed	InstanceId: line vty 0 4
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	swi_008	62.44.96.19	Failed	
Use Defined AAA Methods for Enable Mode Authentication	authentication ble	swi_008	62.44.96.19	Failed	
Use Defined Time Zone	clock timezone	swi_008	62.44.96.19	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	swi_008	62.44.96.19	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	swi_008	62.44.96.19	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	swi_008	62.44.96.19	Failed	
Forbid HTTP Service	no ip http server	swi_008	62.44.96.19	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	swi_008	62.44.96.19	Failed	
Use Defined Logging Buffer Size	logging buffered	swi_008	62.44.96.19	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	swi_008	62.44.96.19	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	swi_008	62.44.96.19	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	swi_008	62.44.96.19	Failed	InstanceId: line con 0

Use Defined SNMP Community Strings and Access Control	snmp-server community	swi_008	62.44.96.19	Failed	Required community string(s) not found Device Detail: ro=bio****; Policy Detail: ro=myr***;
Use Defined Loopback Interface	interface Loopback	swi_008	62.44.96.19	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	swi_008	62.44.96.19	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	swi_008	62.44.96.19	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	swi_008	62.44.96.19	Failed	InstanceId: Vlan3
Bind Logging Service to Loopback Interface	logging source-interface Loopback	swi_008	62.44.96.19	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	swi_008	62.44.96.19	Failed	

Данни за устройство: **su-backbone-sw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	su-backbone-sw	62.44.96.8	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	su-backbone-sw	62.44.96.8	Failed	
Forbid BOOTP Server	no ip bootp server	su-backbone-sw	62.44.96.8	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	su-backbone-sw	62.44.96.8	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	su-backbone-sw	62.44.96.8	Failed	
Use Authenticated NTP	ntp authenticate	su-backbone-sw	62.44.96.8	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	su-backbone-sw	62.44.96.8	Failed	
Use Defined VTY Access Control	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	su-backbone-	62.44.96.8	Failed	InstanceId: Access List:10

List		su-backbone-sw			Policy Detail: ace :=user-input; Device Detail: Severity=debugging;
Use Defined Severity Level for Console Logging	logging console	su-backbone-sw	62.44.96.8	Failed	Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	su-backbone-sw	62.44.96.8	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	su-backbone-sw	62.44.96.8	Failed	
Forbid IP Redirect Message	no ip redirects	su-backbone-sw	62.44.96.8	Failed	InstanceId: Vlan3
Use Defined Logging Buffer Size	logging buffered	su-backbone-sw	62.44.96.8	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Require Encrypted Password for Local Users	username xyz password 7	su-backbone-sw	62.44.96.8	Failed	InstanceId: ach g0l
Forbid Proxy ARP	no ip proxy-arp	su-backbone-sw	62.44.96.8	Failed	InstanceId: Vlan3
Require MOTD Banner	banner motd	su-backbone-sw	62.44.96.8	Failed	
Use Defined Severity Level for Console Logging	logging console	su-backbone-sw	62.44.96.8	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	su-backbone-sw	62.44.96.8	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	su-backbone-sw	62.44.96.8	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	su-backbone-sw	62.44.96.8	Failed	
Use Defined Time Zone	clock timezone	su-backbone-sw	62.44.96.8	Failed	Device Detail: Timezone name=GMT+2; Timezone offset=2; Policy Detail: Timezone name=UTC;Tim

					ezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	su-backbone-sw	62.44.96.8	Failed	InstanceId: Vlan3
Use Defined AAA Servers and Protocols	tacacs-server host	su-backbone-sw	62.44.96.8	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	su-backbone-sw	62.44.96.8	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	su-backbone-sw	62.44.96.8	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	su-backbone-sw	62.44.96.8	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	su-backbone-sw	62.44.96.8	Failed	
Forbid NTP Server service	ntp disable	su-backbone-sw	62.44.96.8	Failed	InstanceId: Vlan3
Use Defined TCP Synwait Time	ip tcp synwait-time	su-backbone-sw	62.44.96.8	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog Servers	logging server	su-backbone-sw	62.44.96.8	Failed	Device Detail: Log Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Use AAA Service	aaa new-model	su-backbone-sw	62.44.96.8	Failed	
Require SSH for Remote Device Access	transport input ssh	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 0 4
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	su-backbone-sw	62.44.96.8	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	su-backbone-sw	62.44.96.8	Failed	
Use Defined Time Zone	clock timezone	su-backbone-sw	62.44.96.8	Failed	Device Detail: Timezone name=GMT+2;

					Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	su-backbone-sw	62.44.96.8	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	su-backbone-sw	62.44.96.8	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	su-backbone-sw	62.44.96.8	Failed	
Use Defined Logging Buffer Size	logging buffered	su-backbone-sw	62.44.96.8	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	su-backbone-sw	62.44.96.8	Failed	InstanceId: line con 0
					Required community string(s) not found
Use Defined SNMP Community Strings and Access Control	snmp-server community	su-backbone-sw	62.44.96.8	Failed	Device Detail: ro=pub*** bio****; Policy Detail: ro=myr***;
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	su-backbone-sw	62.44.96.8	Failed	
Use Defined Loopback Interface	interface Loopback	su-backbone-sw	62.44.96.8	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	su-backbone-sw	62.44.96.8	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	su-backbone-sw	62.44.96.8	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid Defined SNMP Community Strings	no snmp-server community	su-backbone-sw	62.44.96.8	Failed	InstanceId: public
Forbid IP Unreachable	no ip unreachables	su-backbone-	62.44.96.8	Failed	InstanceId: Vlan3

Message		sw			
Bind Logging Service to Loopback Interface	logging source-interface Loopback	su-backbone-sw	62.44.96.8	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	su-backbone-sw	62.44.96.8	Failed	
Use Defined SSH and Telnet Access Control	access-class	su-backbone-sw	62.44.96.8	Failed	InstanceId: line vty 5 15

Данни за устройство:**ucc-sw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	ucc-sw	62.44.109.6	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	ucc-sw	62.44.109.6	Failed	
Forbid BOOTP Server	no ip bootp server	ucc-sw	62.44.109.6	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	ucc-sw	62.44.109.6	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	ucc-sw	62.44.109.6	Failed	
Use Authenticated NTP	ntp authenticate	ucc-sw	62.44.109.6	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	ucc-sw	62.44.109.6	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	ucc-sw	62.44.109.6	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	ucc-sw	62.44.109.6	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	ucc-sw	62.44.109.6	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	ucc-sw	62.44.109.6	Failed	
Forbid IP Redirect Message	no ip redirects	ucc-sw	62.44.109.6	Failed	InstanceId: Vlan109
Use Defined Logging Buffer Size	logging buffered	ucc-sw	62.44.109.6	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;

Require Encrypted Password for Local Users	username xyz password 7	ucc-sw	62.44.109.6	Failed	InstanceId: ach g0l
Forbid Proxy ARP	no ip proxy-arp	ucc-sw	62.44.109.6	Failed	InstanceId: Vlan109
Require MOTD Banner	banner motd	ucc-sw	62.44.109.6	Failed	
Use Defined Severity Level for Console Logging	logging console	ucc-sw	62.44.109.6	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	ucc-sw	62.44.109.6	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	ucc-sw	62.44.109.6	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	ucc-sw	62.44.109.6	Failed	
Use Defined Time Zone	clock timezone	ucc-sw	62.44.109.6	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	ucc-sw	62.44.109.6	Failed	InstanceId: Vlan109
Use Defined AAA Servers and Protocols	tacacs-server host	ucc-sw	62.44.109.6	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	ucc-sw	62.44.109.6	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	ucc-sw	62.44.109.6	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use Defined AAA Methods for User Login Authentication	aaa authentication login	ucc-sw	62.44.109.6	Failed	
Use Defined TCP Synwait Time	ip tcp synwait-time	ucc-sw	62.44.109.6	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog	logging server	ucc-sw	62.44.109.6	Failed	Device Detail:

Servers					Log Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Use AAA-Based Accounting	aaa accounting	ucc-sw	62.44.109.6	Failed	
Forbid NTP Server service	ntp disable	ucc-sw	62.44.109.6	Failed	InstanceId: Vlan109
Use AAA Service	aaa new-model	ucc-sw	62.44.109.6	Failed	
Require SSH for Remote Device Access	transport input ssh	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 0 4
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	ucc-sw	62.44.109.6	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	ucc-sw	62.44.109.6	Failed	
Use Defined Time Zone	clock timezone	ucc-sw	62.44.109.6	Failed	Device Detail: Timezone name=GMT+2 ;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	ucc-sw	62.44.109.6	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	ucc-sw	62.44.109.6	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	ucc-sw	62.44.109.6	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	ucc-sw	62.44.109.6	Failed	
Use Defined Logging Buffer Size	logging buffered	ucc-sw	62.44.109.6	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	ucc-sw	62.44.109.6	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	ucc-sw	62.44.109.6	Failed	InstanceId: line con 0
Use Defined SNMP Community Strings and Access Control	snmp-server community	ucc-sw	62.44.109.6	Failed	Required community string(s) not found Device Detail:

					ro=bio****; Policy Detail: ro=myr***; Loopback interface mismatched or missed.
Use Defined Loopback Interface	interface Loopback	ucc-sw	62.44.109.6	Failed	
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	ucc-sw	62.44.109.6	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	ucc-sw	62.44.109.6	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	ucc-sw	62.44.109.6	Failed	InstanceId: Vlan109
Bind Logging Service to Loopback Interface	logging source-interface Loopback	ucc-sw	62.44.109.6	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	ucc-sw	62.44.109.6	Failed	

Данни за устройство: **middle2-sw**

(Тук ще дам данните само на middle2-sw комутатор - middle4-sw, middle5-sw, mixedn1-sw, north1-sw, north2-sw, north3-sw,north4-sw, rector-sw, south2-sw, south3-sw, south4-sw са с еднакъв хардуерна платформа,една и съща версия на IOS-а и с аналогична конфигурация,по този начин одита за тези устройства ще даде подобни резултати)

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Cisco Express Forwarding	ip cef	middle2-sw	62.44.110.251	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	middle2-sw	62.44.110.251	Failed	
Use Defined Logging Buffer Size	logging buffered	middle2-sw	62.44.110.251	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Use Time Stamps for Debugging Messages	service timestamps debug	middle2-sw	62.44.110.251	Failed	
Forbid Gratuitous ARP	no ip gratuitous-arps	middle2-sw	62.44.110.251	Failed	
Forbid HTTP Service	no ip http server	middle2-sw	62.44.110.251	Failed	

Require TCP-Keepalives-Out Service	service tcp-keepalives-out	middle2-sw	62.44.110.251	Failed	
Require MOTD Banner	banner motd	middle2-sw	62.44.110.251	Failed	
Use Defined Trap Servers	snmp-server host trap server	middle2-sw	62.44.110.251	Failed	
Require Local Users	username xyz password 7	middle2-sw	62.44.110.251	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	middle2-sw	62.44.110.251	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Require Sequence Numbers in Log Messages	service sequence-numbers	middle2-sw	62.44.110.251	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	middle2-sw	62.44.110.251	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	middle2-sw	62.44.110.251	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Require Local Users	username xyz password 7	middle2-sw	62.44.110.251	Failed	
Use AAA-Based Accounting	aaa accounting	middle2-sw	62.44.110.251	Failed	
Forbid CDP	no cdp run	middle2-sw	62.44.110.251	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	middle2-sw	62.44.110.251	Failed	
Use Defined Logging Buffer Size	logging buffered	middle2-sw	62.44.110.251	Failed	Device Detail: Size=empty; Policy Detail: Size=8192; Device Detail: NTP Servers=; Policy Detail: NTP Servers=;
Use Defined NTP Server	ntp server	middle2-sw	62.44.110.251	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	middle2-sw	62.44.110.251	Failed	

Use AAA Service	aaa new-model	middle2-sw	62.44.110.251	Failed	
Forbid PAD Service	no service pad	middle2-sw	62.44.110.251	Failed	
Require Enable Password	enable password	middle2-sw	62.44.110.251	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	middle2-sw	62.44.110.251	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input; Device Detail: Severity=disable; Policy Detail:
Use Defined Severity Level for Console Logging	logging console	middle2-sw	62.44.110.251	Failed	Severity=emergencies;
Forbid BOOTP Server	no ip bootp server	middle2-sw	62.44.110.251	Failed	
Use Defined Severity Level for Console Logging	logging console	middle2-sw	62.44.110.251	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined AAA Servers and Protocols	tacacs-server host	middle2-sw	62.44.110.251	Failed	
Forbid IP Source Routing	no ip source-route	middle2-sw	62.44.110.251	Failed	
Use Defined SNMP Community Strings and Access Control	snmp-server community	middle2-sw	62.44.110.251	Failed	Required community string(s) not found Device Detail: ro=; Policy Detail: ro=myr***;
Use Defined AAA Methods for User Login Authentication	aaa authentication login	middle2-sw	62.44.110.251	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	middle2-sw	62.44.110.251	Failed	
Use Time Stamps for Logging	service timestamps log	middle2-sw	62.44.110.251	Failed	
Bind TACACS+	ip tacacs source-interface	middle2-sw	62.44.110.251	Failed	

Service to Loopback Interface Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	middle2-sw	62.44.110.251	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined TCP Synwait Time	ip tcp synwait-time	middle2-sw	62.44.110.251	Failed	
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	middle2-sw	62.44.110.251	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	middle2-sw	62.44.110.251	Failed	
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	middle2-sw	62.44.110.251	Failed	
Use Defined Loopback Interface	interface Loopback	middle2-sw	62.44.110.251	Failed	
Require Password Encryption Service	service password-encryption	middle2-sw	62.44.110.251	Failed	
Use Defined Syslog Servers	logging server	middle2-sw	62.44.110.251	Failed	Device Detail: Log Servers= Not defined; Policy Detail: Log Servers= Any is ok;
Bind Logging Service to Loopback Interface	logging source-interface Loopback	middle2-sw	62.44.110.251	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	middle2-sw	62.44.110.251	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Authenticated NTP	ntp authenticate	middle2-sw	62.44.110.251	Failed	
Use Defined AAA	aaa authentication enable	middle2-sw	62.44.110.251	Failed	

Methods for Enable Mode Authentication					
Require TCP-Keepalives-In Service	service tcp-keepalives-in	middle2-sw	62.44.110.251	Failed	

Данни за устройство: **rec-gw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	rec-gw	62.44.110.2	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Forbid UDP Small Servers Service	no service udp-small-servers	rec-gw	62.44.110.2	Failed	
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	rec-gw	62.44.110.2	Failed	
Forbid BOOTP Server	no ip bootp server	rec-gw	62.44.110.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-gw	62.44.110.2	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	rec-gw	62.44.110.2	Failed	
Use Authenticated NTP	ntp authenticate	rec-gw	62.44.110.2	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	rec-gw	62.44.110.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	rec-gw	62.44.110.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input; Device Detail: Severity=disable;
Use Defined Severity Level for Console Logging	logging console	rec-gw	62.44.110.2	Failed	Policy Detail: Severity=emergencies ;
Forbid IP Source Routing	no ip source-route	rec-gw	62.44.110.2	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	rec-gw	62.44.110.2	Failed	
Forbid IP Redirect Message	no ip redirects	rec-gw	62.44.110.2	Failed	InstanceId: Serial1
Forbid IP Redirect Message	no ip redirects	rec-gw	62.44.110.2	Failed	InstanceId: Serial0
Forbid IP	no ip redirects	rec-gw	62.44.110.2	Failed	InstanceId: Ethernet0

Redirect Message					
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line vty 2 4
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line vty 0 1
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line con 0
Forbid CDP	no cdp run	rec-gw	62.44.110.2	Failed	
Use Defined Logging Buffer Size	logging buffered	rec-gw	62.44.110.2	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line vty 2 4
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line vty 0 1
Use Defined Timeout for Login Sessions	exec-timeout	rec-gw	62.44.110.2	Failed	InstanceId: line con 0
Require Encrypted Password for Local Users	username xyz password 7	rec-gw	62.44.110.2	Failed	InstanceId: ach g0l<or8Re
Forbid Proxy ARP	no ip proxy-arp	rec-gw	62.44.110.2	Failed	InstanceId: Serial1
Forbid Proxy ARP	no ip proxy-arp	rec-gw	62.44.110.2	Failed	InstanceId: Serial0
Forbid Proxy ARP	no ip proxy-arp	rec-gw	62.44.110.2	Failed	InstanceId: Ethernet0
Require MOTD Banner	banner motd	rec-gw	62.44.110.2	Failed	
Use Defined Severity Level for Console Logging	logging console	rec-gw	62.44.110.2	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	rec-gw	62.44.110.2	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	rec-gw	62.44.110.2	Failed	InstanceId: line vty 2 4
Use Defined SSH and Telnet Access Control	access-class	rec-gw	62.44.110.2	Failed	InstanceId: line vty 0 1
Forbid Summer Time Clock	no clock summer-time	rec-gw	62.44.110.2	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	rec-gw	62.44.110.2	Failed	
Use Defined Time Zone	clock timezone	rec-gw	62.44.110.2	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2;

					Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-gw	62.44.110.2	Failed	InstanceId: Serial1
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-gw	62.44.110.2	Failed	InstanceId: Serial0
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-gw	62.44.110.2	Failed	InstanceId: Ethernet0
Use Defined AAA Servers and Protocols	tacacs-server host	rec-gw	62.44.110.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-gw	62.44.110.2	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	rec-gw	62.44.110.2	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	rec-gw	62.44.110.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-gw	62.44.110.2	Failed	
Forbid NTP Server service	ntp disable	rec-gw	62.44.110.2	Failed	InstanceId: Serial1
Forbid NTP Server service	ntp disable	rec-gw	62.44.110.2	Failed	InstanceId: Serial0
Forbid NTP Server service	ntp disable	rec-gw	62.44.110.2	Failed	InstanceId: Ethernet0
Use Defined TCP Synwait Time	ip tcp synwait-time	rec-gw	62.44.110.2	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Forbid Auxiliary Port	no exec	rec-gw	62.44.110.2	Failed	
Use AAA Service	aaa new-model	rec-gw	62.44.110.2	Failed	
Require SSH for Remote Device Access	transport input ssh	rec-gw	62.44.110.2	Failed	InstanceId: line vty 2 4
Require SSH for Remote Device Access	transport input ssh	rec-gw	62.44.110.2	Failed	InstanceId: line vty 0 1
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-gw	62.44.110.2	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-gw	62.44.110.2	Failed	
Forbid PAD Service	no service pad	rec-gw	62.44.110.2	Failed	
Use Defined	clock timezone	rec-gw	62.44.110.2	Failed	Device Detail:

Time Zone					Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Forbid TCP Small Servers Service	no service tcp-small-servers	rec-gw	62.44.110.2	Failed	
Bind TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	rec-gw	62.44.110.2	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	rec-gw	62.44.110.2	Failed	
Forbid HTTP Service	no ip http server	rec-gw	62.44.110.2	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-gw	62.44.110.2	Failed	
Use Defined Logging Buffer Size	logging buffered	rec-gw	62.44.110.2	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	rec-gw	62.44.110.2	Failed	InstanceId: line vty 2 4
Require Encrypted Line Password	(config-line)#password 7	rec-gw	62.44.110.2	Failed	InstanceId: line vty 0 1
Use Defined SNMP Community Strings and Access Control	snmp-server community	rec-gw	62.44.110.2	Failed	Required community string(s) not found Device Detail: ro=JOTU**** bio****; Policy Detail: ro=myr***;
Use Defined Loopback Interface	interface Loopback	rec-gw	62.44.110.2	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	rec-gw	62.44.110.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_ MASK	rec-gw	62.44.110.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	rec-gw	62.44.110.2	Failed	InstanceId: Serial1
Forbid IP Unreachable Message	no ip unreachables	rec-gw	62.44.110.2	Failed	InstanceId: Serial0
Forbid IP Unreachable Message	no ip unreachables	rec-gw	62.44.110.2	Failed	InstanceId: Ethernet0
Bind Logging Service to	logging source-interface Loopback	rec-gw	62.44.110.2	Failed	

Loopback Interface Require TCP-Keepalives-Out Service	service tcp-keepalives-out	rec-gw	62.44.110.2	Failed	

Данни за устройство: **rec-l3sw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	rec-l3sw	62.44.110.3	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	rec-l3sw	62.44.110.3	Failed	
Forbid BOOTP Server	no ip bootp server	rec-l3sw	62.44.110.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-l3sw	62.44.110.3	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	rec-l3sw	62.44.110.3	Failed	
Use Authenticated NTP	ntp authenticate	rec-l3sw	62.44.110.3	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	rec-l3sw	62.44.110.3	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	rec-l3sw	62.44.110.3	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	rec-l3sw	62.44.110.3	Failed	Device Detail: Severity=disable; Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	rec-l3sw	62.44.110.3	Failed	
Require Password Encryption Service	service password-encryption	rec-l3sw	62.44.110.3	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	rec-l3sw	62.44.110.3	Failed	
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192

Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan110
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24
Forbid IP Redirect Message	no ip redirects	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7
Use Defined Logging Buffer Size	logging buffered	rec-l3sw	62.44.110.3	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Require Encrypted Password for Local Users	username xyz password 7	rec-l3sw	62.44.110.3	Failed	InstanceId: ach get clear time g0l
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan110
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24
Forbid Proxy ARP	no ip proxy-arp	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7
Require MOTD Banner	banner motd	rec-l3sw	62.44.110.3	Failed	
Use Defined Severity Level for Console Logging	logging console	rec-l3sw	62.44.110.3	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	rec-l3sw	62.44.110.3	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 0 4
Forbid	no clock summer-time	rec-l3sw	62.44.110.3	Failed	

Summer Time Clock Require Sequence Numbers in Log Messages	service sequence-numbers	rec-l3sw	62.44.110.3	Failed	
Use Defined Time Zone	clock timezone	rec-l3sw	62.44.110.3	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan110
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7
Use Defined AAA Servers and Protocols	tacacs-server host	rec-l3sw	62.44.110.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-l3sw	62.44.110.3	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	rec-l3sw	62.44.110.3	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	rec-l3sw	62.44.110.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	rec-l3sw	62.44.110.3	Failed	
Forbid NTP Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192
Forbid NTP Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118
Forbid NTP	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114

Server service Forbid NTP Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112
Server service Forbid NTP Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan110
Server service Forbid NTP Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24
Server service	ntp disable	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7
Use Defined TCP Synwait Time	ip tcp synwait-time	rec-l3sw	62.44.110.3	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Require SSH for Remote Device Access	transport input ssh	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 0 4
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112 Policy Detail: ace =10.0.0.0 0.255.255.255;ace

Traffic					=172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255; InstanceId: Vlan110 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	
Use AAA Service	aaa new-model	rec-l3sw	62.44.110.3	Failed	
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-l3sw	62.44.110.3	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-l3sw	62.44.110.3	Failed	
Use Defined Time Zone	clock timezone	rec-l3sw	62.44.110.3	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers	snmp-server host trap server	rec-l3sw	62.44.110.3	Failed	
Bind	ip tacacs source-interface	rec-l3sw	62.44.110.3	Failed	

TACACS+ Service to Loopback Interface	Loopback				
Require TCP-Keepalives-In Service	service tcp-keepalives-in	rec-l3sw	62.44.110.3	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	rec-l3sw	62.44.110.3	Failed	
Use Defined Logging Buffer Size	logging buffered	rec-l3sw	62.44.110.3	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	rec-l3sw	62.44.110.3	Failed	InstanceId: line con 0
Use Defined SNMP Community Strings and Access Control	snmp-server community	rec-l3sw	62.44.110.3	Failed	Required community string(s) not found Device Detail: ro=EXTt**** bio****; Policy Detail: ro=myr***;
Use Defined Loopback Interface	interface Loopback	rec-l3sw	62.44.110.3	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	rec-l3sw	62.44.110.3	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	rec-l3sw	62.44.110.3	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan192
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan118
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan114
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan112
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: Vlan110

Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/24
Forbid IP Unreachable Message	no ip unreachables	rec-l3sw	62.44.110.3	Failed	InstanceId: FastEthernet0/7
Bind Logging Service to Loopback Interface	logging source-interface Loopback	rec-l3sw	62.44.110.3	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	rec-l3sw	62.44.110.3	Failed	
Use Defined SSH and Telnet Access Control	access-class	rec-l3sw	62.44.110.3	Failed	InstanceId: line vty 5 15

Данни за устройство: **iv-l3sw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	iv-l3sw	62.44.120.3	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	iv-l3sw	62.44.120.3	Failed	
Forbid BOOTP Server	no ip bootp server	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-l3sw	62.44.120.3	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	iv-l3sw	62.44.120.3	Failed	
Use Authenticated NTP	ntp authenticate	iv-l3sw	62.44.120.3	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	iv-l3sw	62.44.120.3	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	iv-l3sw	62.44.120.3	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	iv-l3sw	62.44.120.3	Failed	Device Detail: Severity=disable; Policy Detail: Severity=emergencies;
Forbid IP Source Routing	no ip source-route	iv-l3sw	62.44.120.3	Failed	
Require Password	service password-encryption	iv-l3sw	62.44.120.3	Failed	

Encryption Service					
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	iv-l3sw	62.44.120.3	Failed	
Forbid IP Redirect Message	no ip redirects	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120
Forbid IP Redirect Message	no ip redirects	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/15
Forbid IP Redirect Message	no ip redirects	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7
Use Defined Logging Buffer Size	logging buffered	iv-l3sw	62.44.120.3	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Require Encrypted Password for Local Users	username xyz password 7	iv-l3sw	62.44.120.3	Failed	InstanceId: ach get clear time g0l
Forbid Proxy ARP	no ip proxy-arp	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120
Forbid Proxy ARP	no ip proxy-arp	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/15
Forbid Proxy ARP	no ip proxy-arp	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7
Require MOTD Banner	banner motd	iv-l3sw	62.44.120.3	Failed	
Use Defined Severity Level for Console Logging	logging console	iv-l3sw	62.44.120.3	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	iv-l3sw	62.44.120.3	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	iv-l3sw	62.44.120.3	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	iv-l3sw	62.44.120.3	Failed	
Use Defined Time Zone	clock timezone	iv-l3sw	62.44.120.3	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone

					offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/15
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7
Use Defined AAA Servers and Protocols	tacacs-server host	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-l3sw	62.44.120.3	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	iv-l3sw	62.44.120.3	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-l3sw	62.44.120.3	Failed	
Forbid NTP Server service	ntp disable	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120
Forbid NTP Server service	ntp disable	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/15
Forbid NTP Server service	ntp disable	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7
Use Defined TCP Synwait Time	ip tcp synwait-time	iv-l3sw	62.44.120.3	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use AAA Service	aaa new-model	iv-l3sw	62.44.120.3	Failed	
Require SSH for Remote Device Access	transport input ssh	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 0 4
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound	deny ip RFC 1918	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7 Policy Detail: ace =10.0.0.0

Traffic					0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255; InstanceId: FastEthernet0/1 Policy Detail: ace =10.0.0.0 0.255.255.255;ace =172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Forbid Private Source Addresses on Inbound Traffic	deny ip RFC 1918	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-l3sw	62.44.120.3	Failed	
Use Defined Time Zone	clock timezone	iv-l3sw	62.44.120.3	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers Bind	snmp-server host trap server	iv-l3sw	62.44.120.3	Failed	
TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	iv-l3sw	62.44.120.3	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	iv-l3sw	62.44.120.3	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-l3sw	62.44.120.3	Failed	
Use Defined Logging Buffer Size	logging buffered	iv-l3sw	62.44.120.3	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	iv-l3sw	62.44.120.3	Failed	InstanceId: line vty 0 4

Require Encrypted Line Password	(config-line)#password 7	iv-l3sw	62.44.120.3	Failed	InstanceId: line con 0
Use Defined SNMP Community Strings and Access Control	snmp-server community	iv-l3sw	62.44.120.3	Failed	Required community string(s) not found Device Detail: ro=EXTt**** bio****; Policy Detail: ro=myr***;
Use Defined Loopback Interface	interface Loopback	iv-l3sw	62.44.120.3	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	iv-l3sw	62.44.120.3	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_ MASK	iv-l3sw	62.44.120.3	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	iv-l3sw	62.44.120.3	Failed	InstanceId: Vlan120
Forbid IP Unreachable Message	no ip unreachables	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/15
Forbid IP Unreachable Message	no ip unreachables	iv-l3sw	62.44.120.3	Failed	InstanceId: FastEthernet0/7
Bind Logging Service to Loopback Interface	logging source-interface Loopback	iv-l3sw	62.44.120.3	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	iv-l3sw	62.44.120.3	Failed	

Данни за устройство: **iv-gw**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WIT H_MASK	iv-gw	62.44.120.2	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	iv-gw	62.44.120.2	Failed	
Forbid BOOTP Server	no ip bootp server	iv-gw	62.44.120.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-gw	62.44.120.2	Failed	
Bind NTP Service to	ntp source Loopback	iv-gw	62.44.120.2	Failed	

Loopback Interface					
Use Authenticated NTP	ntp authenticate	iv-gw	62.44.120.2	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	iv-gw	62.44.120.2	Failed	
Use Cisco Express Forwarding	ip cef	iv-gw	62.44.120.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_ MASK	iv-gw	62.44.120.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console Logging	logging console	iv-gw	62.44.120.2	Failed	Device Detail: Severity=disable; Policy Detail: Severity=emergencies;
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	iv-gw	62.44.120.2	Failed	
Forbid External Source Addresses on Outbound Traffic	deny ip RFC2827	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0 Policy Detail: ace =user-input;
Forbid IP Redirect Message	no ip redirects	iv-gw	62.44.120.2	Failed	InstanceId: Serial1
Forbid IP Redirect Message	no ip redirects	iv-gw	62.44.120.2	Failed	InstanceId: Serial0
Forbid CDP	no cdp run	iv-gw	62.44.120.2	Failed	
Use Defined Logging Buffer Size	logging buffered	iv-gw	62.44.120.2	Failed	Device Detail: Size=; Policy Detail: Size=8192;
Forbid IP Redirect Message	no ip redirects	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0
Require Encrypted Password for Local Users	username xyz password 7	iv-gw	62.44.120.2	Failed	InstanceId: ach get clear time g0l
Forbid Proxy ARP	no ip proxy-arp	iv-gw	62.44.120.2	Failed	InstanceId: Serial1
Forbid Proxy ARP	no ip proxy-arp	iv-gw	62.44.120.2	Failed	InstanceId: Serial0
Forbid Proxy ARP	no ip proxy-arp	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0
Require MOTD Banner	banner motd	iv-gw	62.44.120.2	Failed	
Use Defined Severity Level for Console Logging	logging console	iv-gw	62.44.120.2	Failed	Device Detail: Severity=disable; Policy Detail: Severity=critical;
Use Defined SSH and	access-class	iv-gw	62.44.120.2	Failed	InstanceId: line con 0

Telnet Access Control					
Use Defined SSH and Telnet Access Control	access-class	iv-gw	62.44.120.2	Failed	InstanceId: line vty 0 4
Forbid Summer Time Clock	no clock summer-time	iv-gw	62.44.120.2	Failed	
Require Sequence Numbers in Log Messages	service sequence-numbers	iv-gw	62.44.120.2	Failed	
Use Defined Time Zone	clock timezone	iv-gw	62.44.120.2	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	iv-gw	62.44.120.2	Failed	InstanceId: CEF not enabled in device
Use Defined AAA Servers and Protocols	tacacs-server host	iv-gw	62.44.120.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-gw	62.44.120.2	Failed	
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	iv-gw	62.44.120.2	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	iv-gw	62.44.120.2	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	iv-gw	62.44.120.2	Failed	
Forbid NTP Server service	ntp disable	iv-gw	62.44.120.2	Failed	InstanceId: Serial1
Forbid NTP Server service	ntp disable	iv-gw	62.44.120.2	Failed	InstanceId: Serial0
Forbid NTP Server service	ntp disable	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0
Use Defined TCP Synwait Time	ip tcp synwait-time	iv-gw	62.44.120.2	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use AAA Service	aaa new-model	iv-gw	62.44.120.2	Failed	
Require SSH for Remote Device Access	transport input ssh	iv-gw	62.44.120.2	Failed	InstanceId: line vty 0 4
Forbid Private Source Addresses on Inbound	deny ip RFC 1918	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0 Policy Detail: ace =10.0.0.0 0.255.255.255;ace

Traffic					=172.16.0.0 0.15.255.255;ace =192.168.0.0 0.0.255.255;ace =127.0.0.0 0.255.255.255;
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-gw	62.44.120.2	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-gw	62.44.120.2	Failed	
Forbid PAD Service	no service pad	iv-gw	62.44.120.2	Failed	
Use Defined Time Zone	clock timezone	iv-gw	62.44.120.2	Failed	Device Detail: Timezone name=GMT+2;Timezone offset=2; Policy Detail: Timezone name=UTC;Timezone offset=0;
Use Defined Trap Servers Bind	snmp-server host trap server	iv-gw	62.44.120.2	Failed	
TACACS+ Service to Loopback Interface	ip tacacs source-interface Loopback	iv-gw	62.44.120.2	Failed	
Require TCP-Keepalives-In Service	service tcp-keepalives-in	iv-gw	62.44.120.2	Failed	
Forbid HTTP Service	no ip http server	iv-gw	62.44.120.2	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	iv-gw	62.44.120.2	Failed	
Use Defined Logging Buffer Size	logging buffered	iv-gw	62.44.120.2	Failed	Device Detail: Size=; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	iv-gw	62.44.120.2	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	iv-gw	62.44.120.2	Failed	InstanceId: line con 0
Use Defined SNMP Community Strings and Access Control	snmp-server community	iv-gw	62.44.120.2	Failed	Required community string(s) not found Device Detail: ro=EXTt**** Hri*** bio****; Policy Detail: ro=myr***;
Use Defined Loopback	interface Loopback	iv-gw	62.44.120.2	Failed	Loopback interface mismatched or missed.

Interface					
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	iv-gw	62.44.120.2	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	iv-gw	62.44.120.2	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	iv-gw	62.44.120.2	Failed	InstanceId: Serial1
Forbid IP Unreachable Message	no ip unreachables	iv-gw	62.44.120.2	Failed	InstanceId: Serial0
Forbid IP Unreachable Message	no ip unreachables	iv-gw	62.44.120.2	Failed	InstanceId: Ethernet0
Bind Logging Service to Loopback Interface	logging source-interface Loopback	iv-gw	62.44.120.2	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	iv-gw	62.44.120.2	Failed	

Данни за устройство: **wap4 (в сградата на СУ има още 3 wireless access point-а със аналогични конфигурации,съответно wap1, wap2, wap3)**

Policy Name	Alias	Device Name	IP Address	Results	Details
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	wap4	62.44.112.125	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Bind Trap Service to Loopback Interface	snmp-server trap-source Loopback	wap4	62.44.112.125	Failed	
Forbid BOOTP Server	no ip bootp server	wap4	62.44.112.125	Failed	
Bind NTP Service to Loopback Interface	ntp source Loopback	wap4	62.44.112.125	Failed	
Use Authenticated NTP	ntp authenticate	wap4	62.44.112.125	Failed	The device is not configured with NTP authentication.
Forbid Gratuitous ARP	no ip gratuitous-arps	wap4	62.44.112.125	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	wap4	62.44.112.125	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Use Defined Severity Level for Console	logging console	wap4	62.44.112.125	Failed	Device Detail: Severity=debugging; Policy Detail:

Logging					Severity=emergencies;
Forbid IP Source Routing	no ip source-route	wap4	62.44.112.125	Failed	
Bind FTP Service to Loopback Interface	ip ftp source-interface Loopback	wap4	62.44.112.125	Failed	
Forbid IP Redirect Message	no ip redirects	wap4	62.44.112.125	Failed	InstanceId: BVI1
Use Defined NTP Server	ntp server	wap4	62.44.112.125	Failed	Device Detail: NTP Servers=; Policy Detail: NTP Servers=;
Forbid CDP	no cdp run	wap4	62.44.112.125	Failed	
Use Defined Logging Buffer Size	logging buffered	wap4	62.44.112.125	Failed	Device Detail: Size=empty; Policy Detail: Size=8192;
Use Defined SSH Timeout and Authentication Retries	ip ssh {time-out | authentication-retries}	wap4	62.44.112.125	Failed	Device Detail: time-out=;retries=; Policy Detail: time-out=60;retries=2;
Require Encrypted Password for Local Users	username xyz password 7	wap4	62.44.112.125	Failed	InstanceId: stefan g0l
Forbid Proxy ARP	no ip proxy-arp	wap4	62.44.112.125	Failed	InstanceId: BVI1
Require MOTD Banner	banner motd	wap4	62.44.112.125	Failed	
Use Defined Severity Level for Console Logging	logging console	wap4	62.44.112.125	Failed	Device Detail: Severity=debugging; Policy Detail: Severity=critical;
Use Defined SSH and Telnet Access Control	access-class	wap4	62.44.112.125	Failed	InstanceId: line con 0
Use Defined SSH and Telnet Access Control	access-class	wap4	62.44.112.125	Failed	InstanceId: line vty 5 15
Use Defined SSH and Telnet Access Control	access-class	wap4	62.44.112.125	Failed	InstanceId: line vty 0 4
Require Sequence Numbers in Log Messages	service sequence-numbers	wap4	62.44.112.125	Failed	
Use Unicast Reverse Path Forwarding	ip verify source unicast reachable-via	wap4	62.44.112.125	Failed	InstanceId: BVI1
Use Defined	aaa authentication login	wap4	62.44.112.125	Failed	

AAA Methods for User Login Authentication					
Use Defined SNMP Access Control List	access-list SNMP_ACL permit SNMP_ACL_BLOCK_WITH_MASK	wap4	62.44.112.125	Failed	InstanceId: Access List:9 Policy Detail: ace :=user-input;
Use AAA-Based Accounting	aaa accounting	wap4	62.44.112.125	Failed	
Use Defined AAA Methods for User Login Authentication	aaa authentication login	wap4	62.44.112.125	Failed	
Forbid NTP Server service	ntp disable	wap4	62.44.112.125	Failed	InstanceId: BVI1
Use Defined TCP Synwait Time	ip tcp synwait-time	wap4	62.44.112.125	Failed	Device Detail: Synwait Time=30; Policy Detail: Synwait Time=10;
Use Defined Syslog Servers	logging server	wap4	62.44.112.125	Failed	Device Detail: Log Servers=Not defined; Policy Detail: Log Servers=Any is ok;
Require SSH for Remote Device Access	transport input ssh	wap4	62.44.112.125	Failed	InstanceId: line vty 5 15
Require SSH for Remote Device Access	transport input ssh	wap4	62.44.112.125	Failed	InstanceId: line vty 0 4
Require AAA Authentication on Console and VTY Lines	login authentication	wap4	62.44.112.125	Failed	InstanceId: line vty 5 15
Require AAA Authentication on Console and VTY Lines	login authentication	wap4	62.44.112.125	Failed	InstanceId: line vty 0 4
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	wap4	62.44.112.125	Failed	
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	wap4	62.44.112.125	Failed	
Use Defined Trap Servers	snmp-server host trap server	wap4	62.44.112.125	Failed	
Bind TACACS+ Service to Loopback	ip tacacs source-interface Loopback	wap4	62.44.112.125	Failed	

Interface Require TCP-Keepalives-In Service	service tcp-keepalives-in	wap4	62.44.112.125	Failed	
Forbid HTTP Service	no ip http server	wap4	62.44.112.125	Failed	
Use Defined Logging Buffer Size	logging buffered	wap4	62.44.112.125	Failed	Device Detail: Size=empty; Policy Detail: Size=16000;
Require Encrypted Line Password	(config-line)#password 7	wap4	62.44.112.125	Failed	InstanceId: line vty 5 15
Require Encrypted Line Password	(config-line)#password 7	wap4	62.44.112.125	Failed	InstanceId: line vty 0 4
Require Encrypted Line Password	(config-line)#password 7	wap4	62.44.112.125	Failed	InstanceId: line con 0
Use Defined AAA Methods for Enable Mode Authentication	aaa authentication enable	wap4	62.44.112.125	Failed	
Use Defined SNMP Community Strings and Access Control	snmp-server community	wap4	62.44.112.125	Failed	Required community string(s) not found Device Detail: ro=bio****; Policy Detail: ro=myr***;
Use Defined Loopback Interface	interface Loopback	wap4	62.44.112.125	Failed	Loopback interface mismatched or missed.
Forbid IP Unreachable Messages for Null Interface	no ip unreachables	wap4	62.44.112.125	Failed	
Use Defined VTY Access Control List	access-list VTY_ACL permit VTY_ACL_BLOCK_WITH_MASK	wap4	62.44.112.125	Failed	InstanceId: Access List:10 Policy Detail: ace :=user-input;
Forbid IP Unreachable Message	no ip unreachables	wap4	62.44.112.125	Failed	InstanceId: BVI1
Bind Logging Service to Loopback Interface	logging source-interface Loopback	wap4	62.44.112.125	Failed	
Require TCP-Keepalives-Out Service	service tcp-keepalives-out	wap4	62.44.112.125	Failed	

Приложение 2

Уязвимости за IOS 12.1(22)EA10 за Cisco Catalist 2950:

Bug ID	Fixed-in vesion	Status	Severity
CSCec07477 cat2950 reloads by bus error when it receives SNMP polling packet	12.1(19)EA1	Fixed	1
CSCsi92350 Catalyst 2940/2950 reset with signal 10 exception	**1st Found-In** 12.1(22)EA10 ,no other IOS are affected(downgrade to 12.1(22)EA9 recommended)	Fixed	1
CSCdy74233 Unexpected reload when receive ICMP control message	12.1(11)EA1a 12.1(12c)EA1 12.1(22)EA1	Fixed	2
CSCea56745 Deferred frame counted, traffic delayed when duplex set as full	12.1(13)EA1b 12.1(14)EA1	Fixed	2
CSCsb21972 Tracebacks when both WCCP and Netflow are configured	12.2(18.9.20)SX4.1 12.2(30.9)S2 12.2(18)SXF2 12.1(26.3)E 12.1(26)E4	Fixed	2
CSCsi54602 Traffic stopped after port role changed with MST	12.1(20)EA1a 12.1(20)EA1b 12.1(20)EA2 12.1(22)EA1 12.1(22)EA1a 12.1(22)EA1b 12.1(22)EA2 12.1(22)EA3 12.1(22)EA4 12.1(22)EA4a 12.1(22)EA5 12.1(22)EA5a 12.1(22)EA6 12.1(22)EA6a 12.1(22)EA7 12.1(22)EA8 12.1(22)EA8a 12.1(22)EA9 12.1(22)EA10	Fixed	2
CSCsi45840 ARP requests for HSRP virtual IP may fail after switchport cmd is used	12.1(27b)E2 12.2(32.8.11)SX80 12.2(18.9.1)SXF	Open	2
CSCsb19159 Command copy const_nvram:vlan.dat startup-config might crash switch	12.2(18)SXF9 12.2(18.8.5)SXF 12.2(32.8.11)SX68 12.2(18)ZY1	Fixed	2
CSCdu32036 CISCO-CONFIG-COPY-MIB.my does not use	12.1(26.3)E 12.1(26)E4	Fixed	2

access list snmp-server	12.0(5)WC14 12.2(3.4)PB 12.2(3.4)B 12.2(2.2)T 12.2(2.2)S 12.2(2.2)PI 12.2(2.2)M 12.0(27)S4c 12.0(25)SX11		
CSCef47414 VTP code fail to restore vlan database properly	12.2(25.1)EWA 12.2(25)EWA2 12.2(18)SXE 12.2(18)SXD1 12.2(17d)SXB9 12.1(23.2)E	Fixed	3
CSCeb45692 Free space in NVRAM is decreasing each time config is saved	12.1(20)EA1	Fixed	3
CSCsg18288 Enable authentication ignores Tacacs+ configuration in rare situation	Still not fixed	Open	3
CSCsd34759 VTP Version Field DoS	12.2(31)SG 12.2(28)SB7 12.2(25)SEF 12.2(25)SEE1 12.2(25)EWA6 12.2(18.10.22)SX3 12.2(18.1.6)ZU 12.2(18)ZU1 12.2(18)SXF5 12.2(18)SXF4 12.2(18)SXE6 12.2(18)SXD7a	Open	3
CSCee49121 static ARPs dont create adjs when used with routes pointing at intf	12.0(32.2)S4 12.2(25)EWA2 12.3(12.4)T 12.2(26.4)S 12.2(25.1)EWA 12.1(23.1)E 12.1(23)E2	Fixed	3
CSCsd34855 VTP update with a VLAN name >100 characters causes buffer overflow	12.0(5)WC16 12.2(18)SXD7a 12.2(31.4.3)SX11 12.2(31)SB5 12.2(28)SB7 12.2(25)S13 12.2(20)S13 12.2(18.10.27)SX3 12.2(18)SXF5 12.2(18)SXF4 12.2(18)SXE6 12.2(33.0.1)SRB 12.2(33)SRA4 12.2(14)S18 12.1(26)E7 12.1(27b)E1	Open	3

CSCei62762 GRE: IP GRE Tunnel packet with Routing Present Bit not dropped.	12.1(22)EA9 12.0(30)S3t 12.0(30)S2n 12.0(28)W5(32b) 12.1(27b)E 12.1(26)E7 12.1(22)EA8 12.1(19)EO6 12.0(5)WC14 12.0(25)SX11 12.0(26)S6b 12.0(27)S4d 12.0(28)S6 12.0(28)S4c	Fixed	3
CSCec67602 ssh: tb in process_watch_timer when sending big ssh packets	12.0(27.3)S1 12.1(22.2)E 12.2(17d)SXB5 12.3(7.3)M 12.3(7.3)T 12.2(23.1)S1	Fixed	3
CSCsj16294 2950/12.1(22)EA9 - Intermittent traffic drop and console hang.	**1st Found-In** 12.1(22)EA9 (downgrade recommended)	Open	3
CSCsh94352 Route remain after deleted Secondary address on 12.1E train	**1st Found-In** 12.1(26)E8 (no workaround)	Open	3
CSCsh43012 2950 may power cycle with no apparent cause	**1st Found-In** 12.1(22)EA8 (**Workaround:** Set up the switch with a console connection)	Open	3
CSCsb63404 2950: memory leak with cluster-HSRP config	**Fixed-In** 12.1(22)EA7 12.2(25)SEF 12.2(25)SEE	Fixed	3
CSCeh48684 Identification field is 0 in every tacacs packet with SYN	12.1(26)E4 12.2(18)SXF 12.2(25)S13 12.3(14)YM10 12.4(2.2)T 12.4(2.2)M 12.3(8)JEB1.20070523 12.2(29.6)S3 12.2(25)EWA6 12.2(18)SXE4 12.1(26.1)E	Fixed	3
CSCdw56650 Error: The field sets of all the ACEs in a ACL should match	12.1(9)EA1d 12.1(11)EA1 12.1(9)EA1c	Fixed	3

Допълнителни уязвимости за IOS 12.1(22)EA7 , Cisco Catalyst 2950:

CSCin74155 SSHv2:router crashes under heavy load at tcb_isvalid	12.1(22)EA5 12.2(33)SRA3 12.3(9a)BC8 12.3(10.2)T 12.3(10.2)M 12.2(24.2)S1 12.2(17d)SXB1 12.2(18)SXD 12.1(22.3)E	Fixed	2
CSCeh68060 switches stop responding to ssh	12.1(19)EA1d	Open	2
CSCec89172 Memory leak in CDP process	12.1(20)EA1 12.1(19)EA1a	Fixed	2
CSCse24889 Malformed SSH version 2 packets may cause processor memory depletion	12.3(14)YM10 12.3(11)ZB2 12.2(44.3)S 12.2(37)SG 12.2(37)SE 12.2(35)SE4 12.4(9.15)T 12.4(9.15)M 12.4(9)T3 12.4(6)T7 12.4(11)XJ2 12.4(11)T2 12.3(8)ZA1 12.3(8)XX2d 12.2(25)S13	Fixed	2
CSCsb11698 Input Queue Wedge with TACACs	12.2(25)FZ 12.2(35)SE 12.2(32.8.5)SR 12.2(18.10.33)SX3 12.2(25)SEF1 12.2(25)EX1 12.2(25)EY4 12.2(18)S12 12.2(29)SV1 12.2(29a)SV 12.2(18)SXF5 12.2(27)SV4 12.2(27)SBB7 12.2(27)SBB4b 12.2(18)SXD7a 12.2(28)SV1 12.2(27)SV5 12.2(18)SO7 12.2(18)ZU2 12.1(19)EO6	Fixed	2
CSCef67660 sshv2 malform client ignore msg cause demage to router	12.2(25)EW 12.2(18)SXE 12.2(18)SXD4 12.2(18)EW2 12.2(17d)SXB8 12.1(23.3)E 12.1(22)EA5 12.1(22)EA4	Fixed	2

CSCef74800 sshv2 server keep sending pkt back to client	12.1(22)AY1 12.3(4)T12 12.3(4)JA2 12.3(2)XE4 12.3(11.4)T 12.3(11)YF3 12.3(11)XL1 12.3(11)T2 12.2(28.5)SPI6a 12.2(25)EWA 12.2(18)SXE 12.1(26.1)E 12.3(12.4)T1 12.2(27.7)S 12.2(25.1)EWA 12.2(25)SG	Fixed	3
CSCsh79114 Cat2950 reloads when issuing crypto key generate rsa modulus 2048	**1st Found-In** 12.1(22)EA9	Fixed	3
CSCdk24176 Radius dir-request unlisted server authen needs to behave like T+	12.3(7)XI 12.3(5.12)M	Fixed	3
CSCin60549 Password promted twice on enable mode authen when RADIUS is dead	12.0(30)S1 12.2(32.8.36)SRB 12.2(31)SB 12.2(28)ZV2 12.2(28)SB1 12.1(25.4)E 12.0(30.1)S 12.3(7)XI 12.3(5.13)T 12.3(5.13)M	Fixed	3

Допълнителни уязвимости за IOS 12.1(14)EA1 за Cisco Catalist 3550:

CSCds00250 SNMP support for IfTable/ifXTable for vLAN (802.1Q/ISL) subinterface.	12.2(13.3)B 12.2(6.8)B 12.2(15)BW 12.2(15)BX 12.2(15)BZ 12.2(6.8)DA 12.2(6.8a)DA 12.2(6.8)M 12.2(6.8)PB 12.2(3.5)PI 12.2(6.8)PI 12.2(9.4)PI5 12.2(6.8)S 12.2(6.8)T 12.2(6.8)T2 12.2(9.3)T 12.2(15)ZN	Fixed	2
CSCsc41793 %AAAA-3-TIMERNOPER: AAA/ACCT/TIMER: No	12.1(22)EA8 12.1(27b)E	Fixed	3

periodic update but timer set.			
CSCse60733 NAS should not send the state attribute in first acc-req after failover	12.4(11.2)M 12.4(11.2)T 12.3(8)JEB 12.1(22)EA10	Fixed	3
CSCea33481 VSEC: Auth Proxy does not work	12.1(21.4)E 12.1(21.4)EC 12.2(17d)SXB1	Open	3