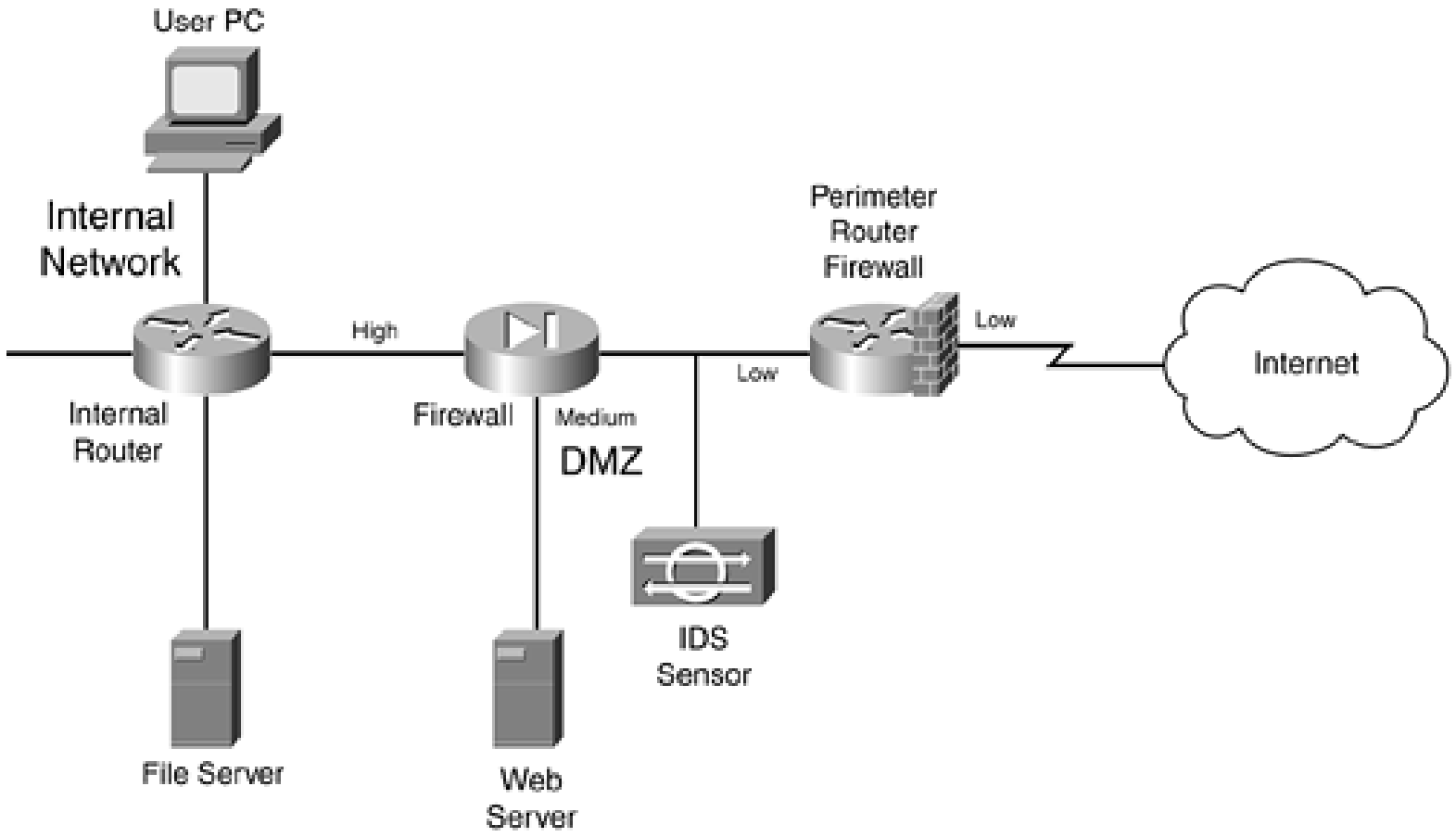
ИТ РЕВИЗИЈА МРЕЖНИХ УРЕЂАЈА

AUDITING NETWORK DEVICES

УРЕЂАЈИ И ПАРАМЕТРИ МРЕЖЕ

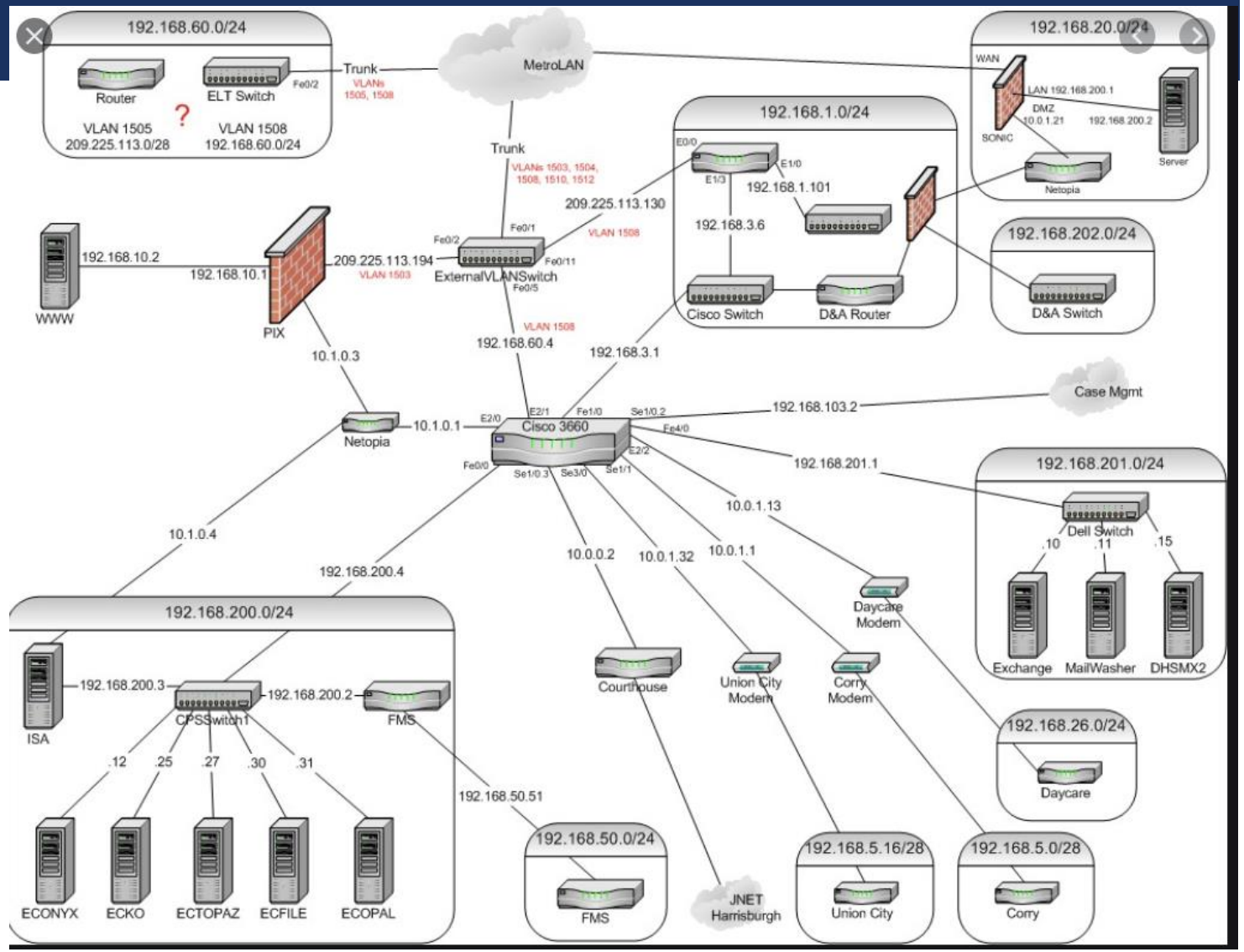
- **Гранични рутери**: Рутери служе као саобраћајни знакови мрежа. Усмеравају саобраћај ка мрежама, ван њих и широм њих. Гранични рутер је последњи рутер под контролом организације пре него што се саобраћај појави на непоузданој мрежи, као што је Интернет.
- **Firewall/Заштитни зидови:** Заштитни зид је уређај који има скуп правила која одређују који саобраћај ће омогућити или забранити да пролази кроз њега. Заштитни зид обично настаје тамо где гранични рутер стаје и чини много темељнији пролаз при филтрирању саобраћаја.
- **Систем за откривање упада (ИДС):** Овај систем функционише као алармни систем за вашу мрежу који се користи за откривање и упозоравање на сумњиве активности. Овај систем може бити изграђен од једног уређаја или колекције сензора постављених на стратешким тачкама мреже.
- **Систем за спречавање упада (ИПС):** У поређењу са традиционалним ИДС-ом који једноставно обавештава администраторе о могућим претњама, ИПС може покушати да аутоматски одбрани циљ без директне интервенције администратора.
- **Демилитаризоване зоне** : ДМЗ се односи на мале мреже које садрже јавне услуге повезане директно на заштитни зид или други уређај за филтрирање и нуде заштиту

МРЕЖЕ


User PC
Internal Network
Perimeter Router Firewall
Low
Internet
High
Low
Internal Router
Firewall
Medium
DMZ
IDS Sensor
File Server
Web Server

МРЕЖЕ

- Најчешће вас чека овако нешто



ПАРАМЕТРИ МРЕЖЕ

- оно што је доступно са интернета
- оно што је видљиво и „споља“ и „изнутра“
- граница између „споља“ и „унутра“
- али – граница није сасвим јасна:

Бежичне мреже, паметни телефони, лаптопови ..

РЕВИЗИЈА РУТЕРА

- Шта је рутер

„ Уређај (или софтвер у рачунару) који изводи функције усмеравања мрежа, према спецификацији OSI layer 3“

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

РЕВИЗИЈА РУТЕРА

Ревизорски поглед

- Рутер је једна „кутија“ у којој се доносе одлуке (*) по правилима која су у складу са претходно утврђеном политиком
- у њему су имплементиране техничке контроле које служе за постизање постављених циљева(*)

(*)везано за ток саобраћаја

ПРИПРЕМА ЗА РЕВИЗИЈУ

- Ко је одговоран?
- Који су циљеви, каква је политика?
- Архитектура
- Контроле (конфигурација рутера)
- Која опрема се користи?
- Да ли је било претходних ревизија и који су били налаз

ИЗВОРИ ИНФОРМАЦИЈА

- Интерни извори
  - Ревизорски тим
  - Систем администратори
  - Мрежни администратори
  - Служба за безбедност информација
  - ИТ безбедност
- произвођачка документација о рутеру
- мрежни дијаграми

- Екстерни извори
  - Објаве произвођача опреме
  - CEERT / CSIRT / CIAC
  - Списак рањивости
  - Најбоље праксе

АРХИТЕКТУРА

- Мора да подржи пословне информационе токове
- Улога рутера у мрежи
  - Interior
  - Border
  - Backbone
- Да ли је гранични рутер једина линија одбране (препоручен концепт заштита по дубини)
- Да ли гранични рутер ради уз постојећи firewall (или више њих)
- Који је ОС?
- Сервисни статус (patch level)?

ПРОЦЕСИ

Важни процеси које **обавезно** треба сагледати :

- Управљање изменама
- Управљање резервним копијама - бекапи
- Управљање корисничким приступом
- Полисе лозинки
- Системске закрпе и ажурирања – patch updates
- Стандардизоване безбедносне поставке / конфигурисања - Standardized secure builds

ИНТЕРВЈУИ, ПРЕГЛЕД ДОКУМЕНТАЦИЈЕ

- Да ли је процес формално дефинисан (процедура)?
- Верификација
- Да ли се процедура поштује
- Да ли се процес заиста одвија „као на папиру“?
- Провера на узорку (обавезно бордер рутер, унутрашњи по случајном узорку)
  - Пример – измена конфигурације Праћење процеса промене – од захтева преко ауторизације до имплементације
  - Реаговање на аларм (да ли је администратор поступио по процедури)
  - Ескалација
- Управљање закрпама

ГРАНИЧНИ РУТЕР

- Гранични рутер има два интерфејса (сваки треба проверити)
- „спољашњи“ и „унутрашњи“

- Његова основна функција је да одлучи о томе да ли ће да одбаци пакет или да га пропусти

- Према правилима која су записана у конфигурационом фајлу који може бити:
  - „STATIC“
  - „STATEFUL“

СТАТИЧКА И STATEFUL ПРАВИЛА

- STATIC:
  - „блокирај сваки саобраћај који долази из приватног адресног опсега“
  - „блокирај сваки СНМП саобраћај“
  - „блокирај долазне пинг захтеве“
  - Итд
- STATEFUL
  - Саобраћај се састоји од низа „питања и одговора“
- Морамо допустити да нам се одговори врате у мрежу али – само одговори на питања која смо заиста поставили Саобраћај се састоји од низа „питања и одговора“
- Морамо допустити да нам се одговори врате у мрежу али – само одговори на питања која смо заиста поставили
- (кондиционали, варијабле)
- Приликом прегледа рута неопходна је помоћ администратора мреже или особа из службе информационе/ ИТ безбедности

ACL (ACCESS CONTROL LIST)

- ACL контролишу саобраћај кроз рутер и могу бити **Static** и **Stateful**

На пример, Cisco ACL могу бити:

- standard ACL (1-99, 1300-1999, source IP only)
- extended ACL (100-199, 2000-2699, all packet parts)
- reflexive ACL (везују „питања и одговоре“)
- named ACL (описни називи уместо бројева)

- Правила се везују за интерфејс (access-group) и за смер саобраћаја (IN/OUT)

СТАТИЧКА ACL

- Да ли се користе сва правила?

Ако не – зашто?

Одговор: „није било таквог саобраћаја...“ (немогуће)

генриши саобраћај и тестирај поново док се не увериш у функционалност листе

- Да ли су најчешће коришћена правила она која се налазе на врху листе?
- ако не , препоручити оптимизацију

УПРАВЉАЊЕ РУТЕРИМА (АДМИНИСТРАЦИЈА)

- Локално (најбоље али није увек изводљиво)
- Удаљено (telnet, SSH, HTTP, SNMP, TFTP)

Безбедност приступа (ако није имплементирано препоручити)

- Засебна мрежа за одржавање мрежних уређаја (management network)
- Шифроване комуникације (SSH, Ipsec)
- Укинути сваки приступ који није неопходан
- Увести временске контроле за неактивност (timeouts)
- Ако нису постављене, увести шифре на приступ преко конзоле

АУТЕНТИКАЦИЈА

- User / password (прегледати листу администратора)
- Администратори морају имати индивидуалне налоге
- Cisco: line mode, user based (old, new)
- Line mode – password (console, AUX, VTY)
- „aaa new-model“ обезбеђује решење за аутентификацију, ауторизацију и accouting
- Централизовано управљање налозима (RADIJUS, TACACS, CISCO management console itd)

SNMP

- Најбоље је искључити га потпуно
- Забранити **read/write community** стрингове
- Забранити **default community** стрингове (**public, private**)
- Ограничити приступ само на одређене адресе (**ACL**)
- Ако се користи, користити последњу верзију (**SNMPv3**, ако је могуће)

НАЈБОЉЕ ПРАКСЕ I

- Забранити сувишне протоколе
  - small tcp/udp (finger, echo, chargen, discard)
  - identd
  - http
  - TFTP
  - tcp keep-alives
  - telnet
  - bootp
  - CDP

НАЈБОЉЕ ПРАКСЕ 2

- Банери - Banners (implementirati)
- Правно обавештење - Legal notice (before logging in)
- Енкриптовање лозинки за приступ
- Безбедно складиштење лозинки
- Безбедно преношење лозинки преко интернета
- Подешавања тачног времена (NTP, clock), подешавање тиме сервера
- Синхронизација
- Подешавање временске зоне за логгинг
- Зимско/Летње рачунање времена

НАЈБОЉЕ ПРАКСЕ 3

Управљање логовима

- Укључити бележење логова
- Syslog сервери – управљање логовима
- Time stamps in msec
- Time zone in stamps
- Верификација величине бафера за прикупљање логова
- Верификација логовања на нивоу конзоле
- Подешавање нивоа логовања
- Заштита рутирања саобраћаја
  - Directed broadcasts (smurf attacks)
  - Source routing (allows specification of your own route)
  - Proxy ARP
  - Tunneled interfaces
  - ICMP redirects (anyone cloud change our routing)
  - ICMP unreachables (leaks too much info)

ПРИМЕРИ КОНТРОЛНЕ ЛИСТЕ

- Преглед процеса администрације рутера
- Преглед банера
- Преглед clock/NTP подешавања
- Преглед подешавања процеса за прикупљање логова
- Преглед AAA активности (Authentication, Authorization, Accounting)
- Провера да ли су сви непотребни сервиси онемогућени/ искључени
- Преглед имплементиране заштите за direct broadcasts, source routing, proxy ARP, tunneled interfaces
- Провера дозвољених ICMP порука (Поруке за дијагностику које настају у случају грешака у ИП повезаним процесима)
- Провера долазних и одлазних ACL-ова
- Спровођење техничке валидације итд…

ПРОВЕРА ACL

- Да ли су примењени филтери по процедури?
- Да ли је ACL ауторизована по процедури?
- Да ли је ACL документована (постоји у мрежној шеми, прате промене у архитектури мреже, уклоњене сервери или радне станице који се не користе)
- Да ли је ACL оптимализована?
- Да ли се спроводи преглед правила у ACL како би се искључила она која више нису потребна
- Алати које се могу користити
  - RAT (router audit tool)
  - Nipper
  - Cisco Config Security Audit Tool (http://ccsat.sourceforge.net)
  - RANCID

ВЕКАР

- Да ли ради бекап конфигурационих фајлова?
- Када је урађен последњи бекап? (после сваке промене)
- Уколико постоје резервни или станд-бу уређаји, проверите да ли бекап може да се примени

РЕВИЗИЈА FIREWALL (ЗАШТИТНОГ ЗИДА)

- Шта је Firewall?

„ Firewall је уређај који се користи за спровођење безбедносних политика унутар мреже или између мрежа контролом протока саобраћаја“

- Има много различитих типова
  - (stateful) packet filtering fw
  - application fw
  - (proxy, reverse proxy..)
  - („deep“) packet inspection fw
  - WAF (web application fw)
  - UTM (unified treath management), itd

РЕВИЗИЈА FIREWALL (ЗАШТИТНОГ ЗИДА)

- Ревизорски поглед:

Firewall је једна „кутија" у којој се доносе одлуке по правилима која су у складу са претходно утврђеном политиком ИТ безбедности

- У њему су имплементиране техничке контроле (рулесетс) које служе за постизање постављених циљева
- Са ревизорске тачке гледишта, ревизија рутера и фиревалл су врло слични; припрема и поступак ревизије се у великој мери подударају
- Технички , могу да буду врло различити , што утиче на ревизију, посебно у делу тестирања и верификовања
- Техничке контроле имају другачије циљеве и различиту имплементацију – доста сложенију него роутер
- Архитектура је такође врло различита

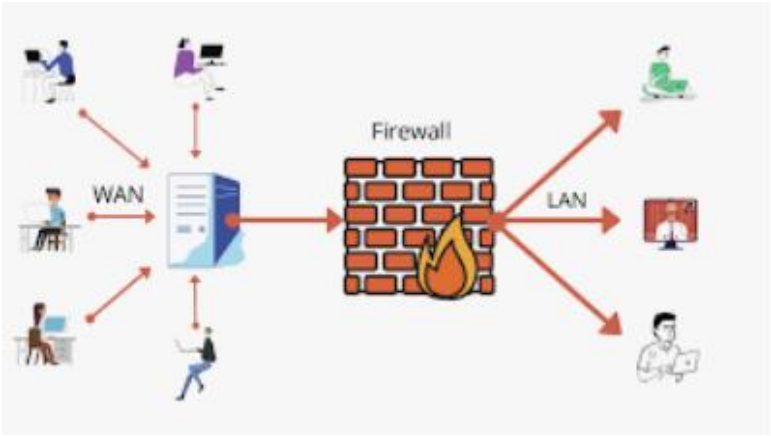
ПРИПРЕМА

- Ко је одговоран?
- Који су циљеви, каква је политика?
- Архитектура
- Контроле (конфигурација firewall)
- Која опрема се користи? (произвођач и модел)
- Да ли је било претходних ревизија и који су били налази?

- Вероватно ће лица одговорна за фиревалл бити иста као и лица одговорна за рутере

АРХИТЕКТУРА

- Знатно сложенија у односу на роутер
- Defense in depth – вишеслојна заштита, већи број firewall-a
- различитих типова, различитим улогама – циљевима и контролама
- NAT / PAT
- Мреже често имају више од једног firewall-a
- Сваки од њих има више мрежних интерфејса
- Правила за обликовање саобраћаја су сложенија



ПОЈМОВИ ВЕЗАНИ ЗА FIREWALL

- Packet filter – static / stateful (као код рутера)
- Proxy
- Reverse proxy
- Deep packet inspection
- Application firewall
- Unified threat management
- NAT / PAT (prevođenje RFC1918 адреса у јевне и обратно)
- IDS / IPS

ПОЛИТИКА FIREWALLA

- Да ли је политиком компаније дефинисано шта фиревалл треба да ради?
- Ако политика није дефинисана разговарамо са менаџментом – каква су очекивања од примена firewall уређаја
- Многи администратори сматрају да је политика записана у самом firewall , на језику којим се пишу правила (fw rules)
- Можемо и одатле да почнемо
- Треба утврдити
  - Које информације штитимо помоћу firewall?
  - Шта све још очекујемо од firewall?
  - Који су укупни ризици, које разлике је организација спремна да прихвати?

ПРОЦЕСИ (ИСТИ КАО ЗА РУТЕР)

- Контрола измена
- Управљање резервним копијама - бекапи
- Управљање корисничким приступом
- Полисе лозинки
- Системске закрпе и ажурирања – patch updatesСтандардизоване безбедносне поставке / конфигурисања - Standardized secure builds

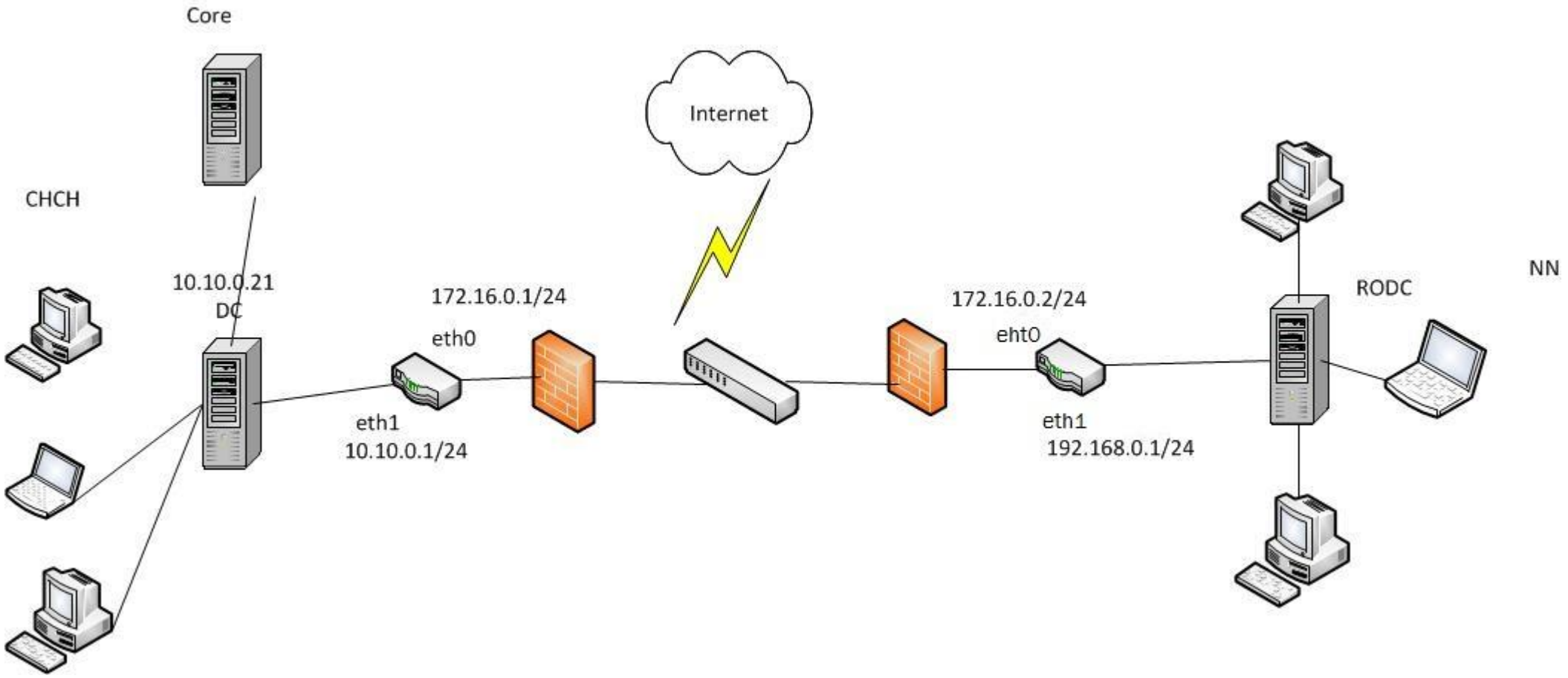
- Интервјуи, преглед корисника, права приступа, преглед документација, прегледи правила

ПРЕГЛЕД АРХИТЕКТУРЕ

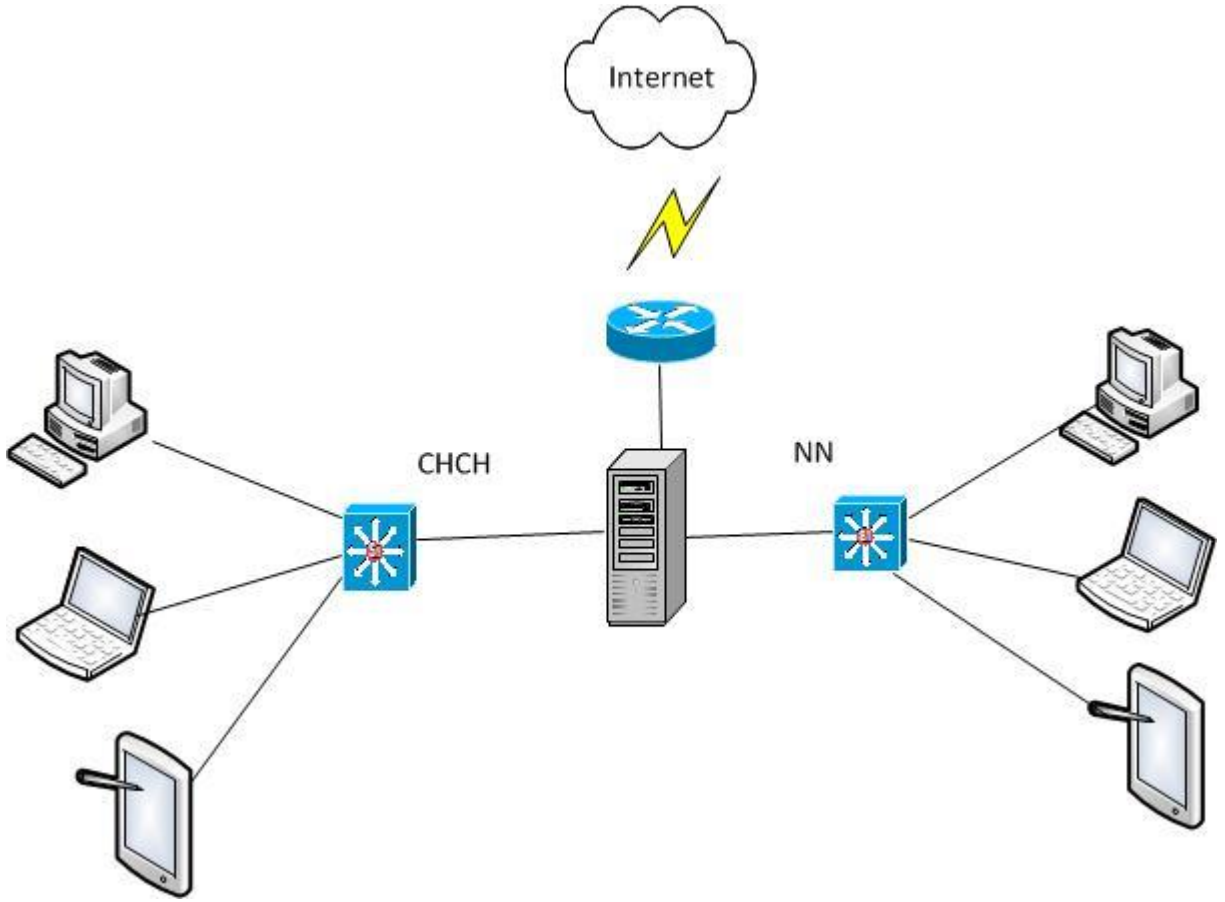
- Утврдити да ли је архитектура у складу са политиком
- Утврдити токове информација
- Дијаграм физичког повезивања (на пример – да ли је више интефејса везано на исти switch? hub?)
- Дијаграм логичког повезивања

- Сврха логичких дијаграма је да прикажу проток информација
- Сврха firewall-a је да контролише проток информација

ЛОГИЧКИ ДИЈАГРАМ



ФИЗИЧКИ ДИЈАГРАМ

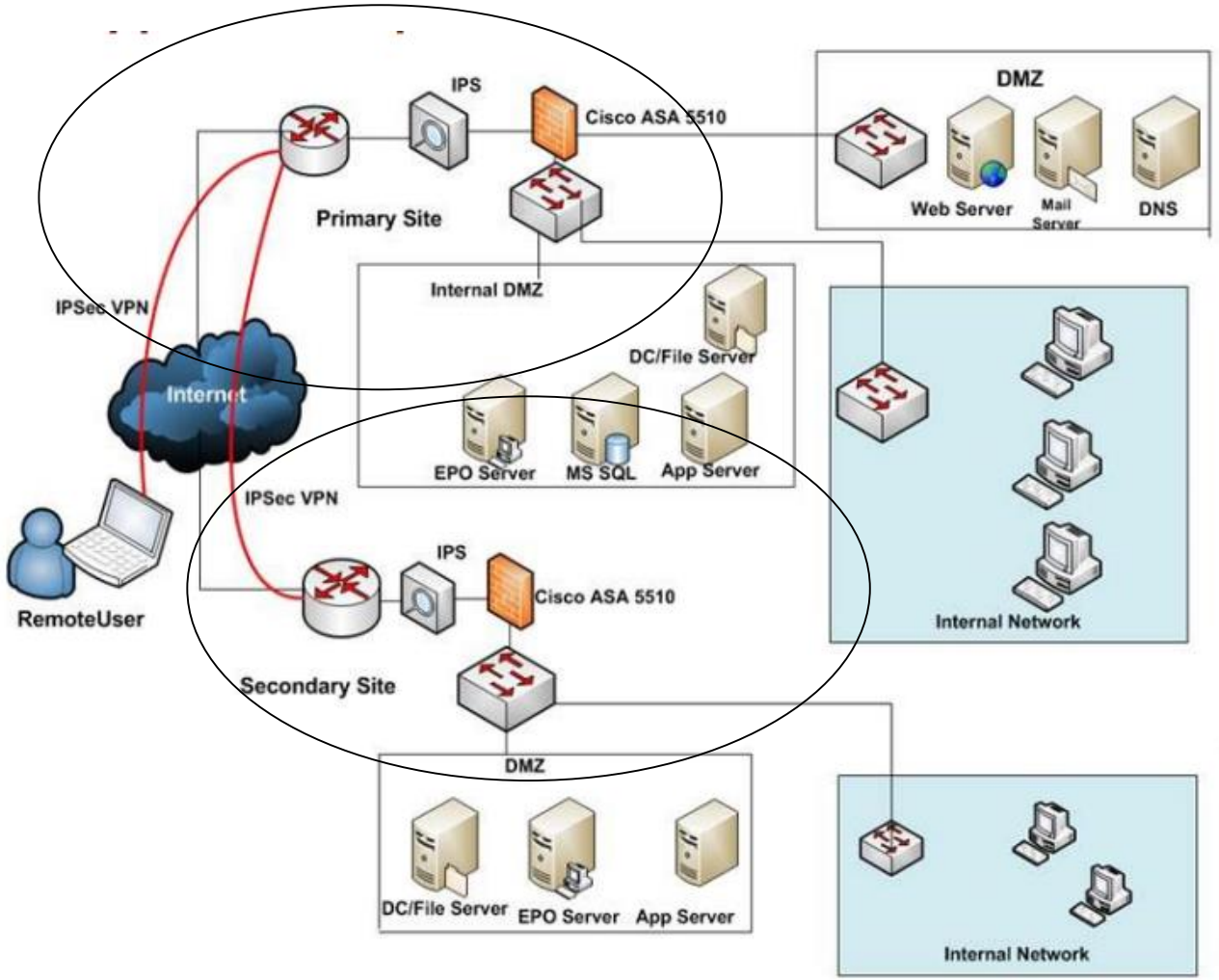


АРХИТЕКТУРА, ПРИМЕРИ I

- Један firewall – без router-а
- Један firewall – са border router-ом
- Двоструки унутрашњи (inline) firewall-и
- Firewall + VPN
- Firewall + VPN + border router + IDS

АРХИТЕКТУРА, ПРИМЕРИ 2

- FW + VPN + IDS



ПЛАТФОРМА

- Платформа – Уређај или Оперативни систем (само softver)?
- Уређај (Appliance)
  - Предности
    - Очекује се да платформе долазе потпуно обезбеђене
    - Дизајн одговара сврси употребе
  - Недостаци
    - Затворене, пропадају компанији која их је направила
    - Морате веровати вендору
- Оперативни систем
  - Предности
    - Већа контрола у процесу обезбеђивања система
    - Изворни код је често доступан уз решење
  - Недостаци
    - Више рада у процесу обезбеђивања система
    - Више прилике да се направи грешка

ВАЛИДАЦИЈА ПРАВИЛА

- Најбоље је урадити мануалну валидацију правила (бар најважнијих јер их може бити на стотине)
- Уклонити непотребна правила (консултације са особама задуженим за безбедност, администратором firewall или архитектом мрежног система)
- Проверите да ли се правила понављају (многа правила могу бити комбинација више правила)
- Идентификујте правила која нису ауторизована
- Уколико је могуће свести систем на најмањи број правила

ВАЛИДАЦИЈА ПРАВИЛА

- Редослед правила треба да буде што једноставнији
- Проверите да ли се превиђају или подразумевају правила („заменити“)
- Проверите да ли постоје правила која имају омогућено логовање (логујте само неопходно)
- Сва правила морају бити документована и одобрена

ВАЛИДАЦИЈА ФИЛТЕРА ПРАВИЛА

- Да ли су филтери правила у складу са политиком?
- Да ли су филтери правила ауторизована?
- Да ли су филтери правила оптимизовани?
- Алати које можете користити
  - Nipper (config parser)
  - Scan through (nmap) and sniff on the other side (tcpdump, wireshark)
  - Hping, nemesis, nessus

ОСНОВНЕ ПРОВЕРЕ

- TCP and UDP scan the FW itself for all 65535 ports
- Check if ICMP echo requests get passed (pingsweep)
- SYN scan subnets for open ports (full TCP for proxies)
- Slow SYN scan to see if port scans are detected
- FIN scan – compare to SYN (if treated differently)
- ACK scan, fragmented ACK scan (compare to SYN / FIN)
- UDP scan subnets
- Scan through firewall
- Listen packets on the other side – see what packets are allowed through
- Scan every network from every interface

ЛОГОВИ И АЛАРМИ

- У току скенирања направили смо велику „буку“
- На крају је потребно проверити шта је остало забележено у лог фајловима
- Да ли су генерисани неки аларми?
- Ко је обавештен?
- Да ли неко редовно прегледа лог фајлове и колико често?
- Да ли је обезбеђен интегритет и доступност логова?

БЕКАП – РЕЗЕРВНЕ КОПИЈЕ (КАО И КОД РУТЕРА)

- Да ли се ради снапсхоот бекап или неки други бекап система?
- Да ли ради бекап конфигурационих фајлова?
- Када је урађен последњи бекап? (после сваке промене)
- Уколико је могуће проверите да ли је бекап валидан (урадите повраћај на пређашње стање)

РЕВИЗИЈА IDS И IPS

- IDS је у основи прислушни уређај (sniffer) који реагује када препозна узорке саобраћаја који се сматрају карактеристичним за разне врсте напада.
- Ти узорци су тзв сигнатуре. Успешност IDS зависи од ажурности сигнатура.
- IPS је IDS којем је функција реаговања проширена. Он не само да генерише упозорење, већ може активно да утиче на правила за обликовање саобраћаја.

ВЕРИФИКАЦИЈА

- Користити нмап за генерисање различитог саобраћаја за скенирање
- Испробати различите брзине (nmap –T option)
- Генеришите разне примере за експлоатацију
- Генеришите фрагментисан саобраћај (fragrouter)
- Генеришите различите величине пакета (DoS)
- Комбиновати са снифером за проверу тачности
- Избројати тест случајеве, избројати добијене алертове – упоредити
- Да ли недостају 2 или 3 или 100 (или више)?

.. И ЈОШ ПРОВЕРА

- Архитектура – NIDS или HIDS?
- Недостају алертови – да ли је ажурирана база потписа (signature base)?
- Како раде лаертови – само логују или шаљу позив/нотификацију?
- Колико често се ажурирају потписи?
- Ко скида и одлучује који потписи ће се применити?
- Ко конфигурише IPS правила? Да ли се тестирају и ауторизују пре пуштања у продукцију?
- Како се поставља – укључује у порт на свичу?

SWITCH

- Switch је уређај који прослеђује саобраћај између својих портова на основу MAC адреса у заглављима етхернет пакета
- Основна функција је да се колизије и ретрансмисије сведу на најмању могућу меру
- Типичан савремени свитцх пружа низ додатних функција: VLAN – virtual LAN
- Ова функционалност уноси безбедносне ризике који се често превиђају

VLAN

- Контрола мрежног саобраћаја – сегментација, trunking
- Исте карактеристике као физичка LAN мрежа
- Омогућава софтверску контролу мрежних конфигурација
- Груписање портова у виртуелне броадцаст домене
- Цео LAN не мора да буде на једном свичу, тј на истој локацији

VTP – VLAN TRUNKING PROTOCOL

- Служи за одржавање конфигурационих параметара
- Централни switch – синхронизација са осталима
- Информације о VLAN мрежама могу се динамички мењати и ажурирати по потреби
- Сваки switch се додељује једном VTP домену
- Сваки VTP мора да има име и password

УЛОГА

- Контрола и ограничавање саобраћаја
- QoS – означавање и приоритизација
- ACL филтери за контролу
- Блокада L2 протокола на одређеним портовима
- Management ports – само у засебним VLAN мрежама
- Контролисана употреба VLAN 1

VLAN 10 - ПРЕПОРУКЕ

- Портови су додељени по дефаулту – представља безбедносни ризик
- Уколико не мора да се корсти – најбоље га не користити
- Скинути VLAN 10 са свих портова који се не користе или нису потребни
- Одвојити саобраћај за управљање од VLAN 10 и наменити други VLAN за то
- Размотрити употребу "оут-оф-банд" начина администрирања (алтернативни приступ за администрирање, а не преко LAN-а)
- VLAN не треба посматрати као безбедносну контролу
- VLAN је сложен концепт који уноси специфичне безбедносне ризике и захтева специфичне контроле
- VLAN треба редовно проверавати и одржавати

РАСПОЛОЖИВИ КОНТРОЛНИ МЕХАНИЗМИ

- VLAN ACL (VACL) – треба да постоје ACL за сваки VLAN, документоване и одобрене
- Port-based ACL (PACL) – уколико се користи мора бити документован и одобрен
- Port security (identify MAC allowed on a port) – препорука да се користи (уколико је могуће)
- Ports can be disabled (препорука, портови који се не користе требају бити искључени)
- Reserved „unused“ VLAN (no traffic, no gateway)
- VLAN trunking restrictions (minimum VLANs)
- DHCP snooping
- ARP inspection

БЕЖИЧНЕ МРЕЖЕ

- (wi-fi, IEEE 802.11)
- Општи приступ је исти као и за претходно споменуто
- Архитектура, топологија
- Идентификовати активну опрему (AP, радио линкове, унутрашње и спољашње антене)
- Има ли одступања у односу на ауторизовано стање (политике, техничка документација)

БЕЖИЧНЕ МРЕЖЕ - СПЕЦИФИЧНОСТИ

- AP (access points) за аутентификацију и размену шифарских кључева имају на располагању многобројне варијанте EAP протокола
- EAP - extensive autentication protocol
- PEAP, TTLS; EAP/TLS, LEAP, EAP-FAST… (око 40 различитих метода)
- EAP се користи за шифровање
- Проверити да ли се користи адекватан метод
- Неки су познати по слабостима (LEAP)
- NIST SP800-120 може да буде користан за евалуацију EAP

БЕЖИЧНЕ МРЕЖЕ – ЕНКРИПЦИЈА И ПРЕПОРУКЕ

- Enkripcija – опције и препоруке
- Wep – wired equivalent privacy
- Изабрати други метод ако је могуће
- Ако не, користити врло дуге лозинке за заштиту кључа
- Често мењајте лозинку
- WEP се веома лако дешифрује – напад је тривијалан и лако доступан

БЕЖИЧНЕ МРЕЖЕ – WPA

- WPA (TKIP)
- изабрати passphrase дужине од 20 знакова
- чувати passphrase за PSK у тајности
- Треба знати да је WPA-PSK првенствено намењен за кућну, а не пословну употребу
- за пословне потребе изабрати WPS/WPA2 са 802.1x/EAP
- WPA2 (CCMP/AES) – counter mode with cipher block chaining message autentication core protocol

БЕЖИЧНЕ МРЕЖЕ – ПРЕПОРУКЕ

- Wireless за кориснике издвојити у засебан сегмент
- Веза са остатком корпоративне мреже : VPN gateway plus FW,
- Употребити SSL, SSH, PPTP…
- Комбиновано са MAC филтерима, стално праћење…
- Не сме се изгубити из вида да wирелесс неконтролисано излази изван граница физичке заштите објекта – ризик од крађе приступа је увек доступан
- Избегавајте да се кроз wireless мрежу омогући приступ базама података, личним подацима или критичним апликацијама (одлука на основу процене ризика)
- За проверу WiFi рутера користите већ описану методологију
- Додатне контроле:
  - Strong authentication and encryption
  - Any defaults (passwords, config settings…)?
  - Restricted management access
  - Session timeouts
  - Снага сигнала
  - Заштита SSID

ХВАЛА