МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ
МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Болдбаатар ДҮҮРЭНЖАРГАЛ

FIREWALL ТӨХӨӨРӨМЖИЙН ТӨРӨЛ, DMZ ХЭРЭГЛЭЭ

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УЛААНБААТАР ХОТ
2020 ОН

МОНГОЛ УЛСЫН БОЛОВСРОЛЫН ИХ СУРГУУЛЬ

МАТЕМАТИК, БАЙГАЛИЙН УХААНЫ СУРГУУЛЬ

МЭДЭЭЛЭЛ ЗҮЙН ТЭНХИМ

Ачит
Болдбаатар ДҮҮРЭНЖАРГАЛ

FIREWALL ТӨХӨӨРӨМЖИЙН ТӨРӨЛ, DMZ ХЭРЭГЛЭЭ

D011401

БАКАЛАВРЫН ДИПЛОМЫН АЖИЛ

УДИРДАГЧ: /Ц.НЯМСҮРЭН/

ШҮҮМЖЛЭГЧ: /Т.УЛАМБАЯР/

УЛААНБААТАР ХОТ
2020 ОН

АГУУЛГА

Хүснэгтийн жагсаалт

Зургийн жагсаалт

УДИРТГАЛ

Сэдвийн үндэслэл

Өнөөгийн сүлжээнүүд хамтарсан үйлдвэр, стратегийн түншлэл гэх мэт бизнесийн шинэ нөхцөл байдалд дасан зохицохын тулд тогтмол өөрчлөгдөн хөгжиж, дотоод сүлжээнүүдийн интернетэд холбогдох түвшин нэмэгдэж байна. Сүлжээ хурдацтай хөгжиж байгаагийн хэрээр аюулгүй байдлыг хамгаалах технологийг хөгжүүлэх шаардлагатай. Дэлхийн эдийн засгийн форумаас жил бүр хамгийн их тохиолддог эрсдэлийг танилцуулдаг билээ. 2018 оны танилцуулгад кибер халдлага, мэдээлэл алдагдах эрсдэлүүдийг онцолсон. Орчин үеийн кибер халдлага банк санхүү, худалдаа үйлчилгээ, үйлдвэрлэл, төрийн байгууллага, интернет дэлгүүр зэрэг бүхий л салбарууд руу чиглэсэн байдаг.

Цар тахлын нөхцөл байдал нь дижитал шилжилтийг улам хурдацтай хөгжихөд нөлөөлсөн билээ. Цар тахалтай холбоотойгоор хүмүүс цахим үйл ажиллагаа явуулах нь ихэссээр байна. Цахим үйл ажиллагаа ихээр явуулах нь гаднын халдлага, аюулын эрсдэлийг нэмэгдүүлж байгаа юм. Интернетэд холбогдсон төхөөрөмжийн тоо, өгөгдөл дамжуулах хурд нэмэгдэж буйг дагаад мэдээлэл алдагдах эрсдэл нэмэгдэнэ. Халдлагын 58% нь жижиг, дунд бизнесийн байгууллагууд руу чиглэдэг. Жижиг дунд бизнес рүү чиглэсэн халдлагуудын 79% нь амжилттай болдог гэсэн судалгаа байна[1]. Байгууллагуудын хувьд халдлагад өртсөнөөр чухал мэдээллээ алдах, үйл ажиллагаа нь удаашрах, үр ашиггүй зардал гэх мэт эрсдэлүүдтэй учрах магадлалтай.Тийм учраас байгууллага болзошгүй эрсдэлээс хамгаалах, сэргийлэх шаардлагатай. Байгууллагын сүлжээнд зайлшгүй байх шаардлагатай анхан шатны хамгаалалт нь firewall (Галт хана) – ын хамгаалалт юм.

Сэдвийн зорилго:

Firewall төхөөрөмжийн талаар судалгаа хийх, Firewall ашиглан DMZ сүлжээ үүсгэж ашиглах тохиргоог виртуал орчинд хийж турших.

Сэдвийн зорилтууд:

- ✓ Сүлжээний Firewall төхөөрөмжийн талаар судлах
- ✓ DMZ -ийн хэрэглээг судлах
- ✓ DMZ-ийн тохиргоог судлах
- ✓ Cisco packet tracer програмд DMZ ашигласан сүлжээ үүсгэж турших

[1] *Naranchuluun, G., 2020. Check Point Firewall. [online] greensoft.mn. Available at: <https://vertexmon.com/checkpoint> [Accessed 20 December 2020]. гаргасан*

БҮЛЭГ I. ОНОЛЫН СУДАЛГААНЫ ХЭСЭГ

1.1 Сүлжээний аюулгүй байдал

Сүлжээний аюулгүй байдал гэдэг нь таны сүлжээ болон өгөгдлийн ашиглалт, бүрэн бүтэн байдлыг хамгаалах зорилготой аливаа үйл ажиллагаа юм.

Сүлжээний аюулгүй байдал нь компьютерын сүлжээ болон сүлжээний нөөцөд хууль бусаар нэвтрэх, зүй бусаар ашиглах, өөрчлөх, үгүйсгэхээс урьдчилан сэргийлэх, хянах бодлого, үйл ажиллагаанаас бүрдэнэ.

Сүлжээний аюулгүй байдлыг бүрдүүлж буй үндсэн ойлголтууд:

1. Нууцлагдсан байдал (confidentiality) - Үйлчилгээ, бүрдэл хэсгүүд болон дэд бүтцийн элементүүд хууль бус нэвтрэлтээс хамгаалагдсан байх, зөвхөн эрх бүхий этгээд хандах боломжийг хангасан байх.
2. Бүрэн бүтэн байдал (Integrity) - Мэдээлэл цаг үедээ нийцсэн, зөрчилдөөнгүй, хууль бусаар, зөвшөөрөлгүй өөрчлөх, нөлөөлөхөөс хамгаалагдсан байх
3. Хүртээмжтэй байдал (availability) - Мэдээллийн нөөц, үйлчилгээг хүссэн үедээ, дурын цэгээс ашиглах боломж

Сүлжээнд холбогдсон бүх тоног төхөөрөмж, дамжиж буй өгөгдөл мэдээлэл, тэнд ажиллаж буй хүмүүсийг сүлжээний орчин гэдэг. Энэ орчинд эрх олгогдоогүй этгээд хандах боломжгүй, тоног төхөөрөмжийн тохируулга, дамжиж буй өгөгдлийг зүй бусаар өөрчлөх боломжгүй, хандах ёстой этгээд хэзээд ч хандах боломжтой байхыг НБХ гэж үзнэ. Сүлжээний аюулгүй байдлыг хангахын тулд эрсдэонлийн үнэлгээн дээр тулгуурлан НБХ-г хангахад чиглэсэн төрөл бүрийн хяналтыг хэрэгжүүлж, байгууллагын удирдлагын баталсан зөвшөөрөлгүй хандалт, ашиглалт, зүй бус үйлдлүүдтэй холбоотой аюулгүй байдлын бодлого журмыг баталж мөрдүүлдэг. Сүлжээний администраторын зөвшөөрлийн дагуу сүлжээн дэх хэрэглэгчид сүлжээнд оногдсон нэвтрэх эрхээр хандаж сүлжээний нөөц мэдээллийг авах, ашиглах боломжтой.

Сүлжээ хэмээх ухагдахуунд өдөр тутмын үйл ажиллагаанд ашиглагдах дотоод, болон гадаад бүх төрлийн сүлжээ хамаарагдана.

- WAN - бүх нийтийг хамарсан сүлжээ
- MAN - тодорхой бүс нутгийг хамарсан сүлжээ
- LAN - тухайн байгууллага, барилга, дэд бүтцийг хамарсан сүлжээ гэсэн ангилал байдаг.

Сүлжээний аюул занал

Сүлжээний аюул занал гэдэг нь систем болон байгууллагад хор учруулж болох сүлжээний аюулгүй байдлыг ямар нэг байдлаар зөрчиж болох боломж, үйлдэл, үйл явдлыг хэлдэг. Аливаа аюул занал тохиолдлын чанартай аль эсвэл тодорхой ашиг сонирхол, төлөвлөгөөний дагуу үүссэн байж болдог. Хэрэв тухайн нөхцөл байдалд ямарваа нэг гэмтэл системийн алдаа аль эсвэл байгалийн гамшгаас үүдэлтэй аюул тохиолдвол түүнийг санаатай буюу санамсаргүй гэж тодорхойлно.

Аюул гэдэг нь мэдээллийн систем, сүлжээний аюулгүй байдлыг зөрчиж, эвдэж чадах үйлдэл, үйл явц юм. Гурван бүрдэл хэсэгтэй:

1. Бай. Довтолгоонд өртөж буй бүрдэл хэсэг
2. Агентууд. Аюул, заналхийлэл агуулж, учруулж буй субъект
3. Үйл явдал. Аюул агуулж буй үйлдэл

Сүлжээний эмзэг байдал, цоорхой гэдэгт Байгууллагын сүлжээний орчин, түүний удирдлага, зохион байгуулалтайд оршин буй аюул заналыг хэрэгжүүлэхэд ашиглаж болох зам, суваг, цоорхойг хамгаалалтгүй байдлыг ойлгоно. Аюул заналтай зайлшгүй холбоотой урган гарч ирдэг нэг ойлголт нь эмзэг байдал, цоорхой (vulnerability) юм.

- Довтолгоон үйлдэж болох боломжит зам, суваг
- Интернетийн холболт
- Алсын зайнаас хандах цэгүүд
- Бусад байгууллагатай холбогдсон холболт
- Биет байдлаар нэвтрэн орох цэгүүд
- Хэрэглэгчийн хандах цэгүүд
- Утасгүй холбооны сүлжээний хандалтын цэгүүд.

Сүлжээний аюул занал, эмзэг байдлын хослолоос сүлжээний эрсдэл үүснэ. Сүлжээний эрсдэл гэж сүлжээний эмзэг байдал, цоорхойг ашиглан аюул заналыг хэрэгжүүлж хор хохирол учруулж болох магадлалыг ойлгоно.

Эрсдэлийн төрлүүд

- Програм хангамж болон техник хангамжийн эрсдэл
- Ажиллагсдын мэргэжлийн болон хувь хүний ёс суртахуунаас үүсэх эрсдэл
- Ажилтнуудын компьютер болон аюулгүй ажиллагааны хангалттай бус мэдлэгтэй холбоотой эрсдэл
- Интернет болон электрон шуудангийн эрсдэлүүд
- Дотоод гадаад сүлжээний эрсдэлүүд
- Мэдээлэл дамжуулалт, холбооны технологийн эрсдэл
- Мэдээлэл хадгалалт, тээвэрлэлтээс үүдэх эрсдэл
- Мэдээлэл санаатай болон санамсаргүй алдагдах эрсдэл
- Байгалийн гамшгийн эрсдэл
- Өрсөлдөгчийн тагнуулын үйл ажиллагаанаас үүдэх эрсдэл
- Мэдээллийн дайн буюу кибер терроризмын эрсдэл зэрэг эрсдэлүүд

Эрсдэлд нөлөөлөх хүчин зүйл

Хүний хүчин зүйл : Санаатай болон санамсаргүй

Санаатай – Компьютерийн гэмт хэрэг үйлдэгчид буюу хакер кракер, өрсөлдөгчид, буруу санасан хамтрагч , байгууллагын зарим ажилтнуудын зүй бус ажиллагаа.

Санамсаргүй – Компьютерийн талаар мэдлэг чадвар дутмаг байдлаас болж баталгаагүй мэдээлэл татаж авах, өөрсдийн болгоомжгүйгээс хулгайд алдах.

Техникийн хүчин зүйл:

Чанаргүй тоног төхөөрөмж, хамгаалалтын програм хангамж, хэрэгсэл, холбоо , хамгаалалт, дохиоллын техник хэрэгслүүд, аюултай үйлдвэрлэл, тээвэрлэлт, хадгалалт.

Байгалийн хүчин зүйл:

Газар хөдлөлт, үер, хар салхи зэрэг байгалийн гамшгууд.

Халдлага гэдэг бол эмзэг байдлыг ашиглан хор хохирол учруулах оролдлого. Гаднын халдагч этгээдийн эртнээс төлөвлөсөн ашиг сонирхлын үүднээс үйл ажиллагаанд саад хийвэл түүнийг төвлөрсөн аюул занал буюу халдлага гэж тодорхойлно.

ТӨРӨЛ:

- Гаднын халдлага
- Дотоод халдлага

1.1.1 Сүлжээний аюулгүй байдлын хэлбэрүүд

Физик аюулгүй байдал

Сүлжээний аюулгүй байдлын хувьд яригдах хамгийн гол асуудлын нэг бол физик аюулгүй байдал. Физик аюулгүй байдал нь тухайн сүлжээн дэх нөөц, төхөөрөмжид халдах, гэмтэл учруулах, хулгайд алдагдах гэх мэт биет байдлаар халдах аюулгүй байдлын хэмжигдэхүүнээр илэрхийлэгдэнэ. Мэдээллийг зөвшөөрөлгүй авах хамгийн түгээмэл арга нь тухайн байгууллагын сүлжээний төхөөрөмжийг хулгайлах. Энэ нь тус сүлжээний шаардлагатай бүх мэдээллийг хадгалсан байдаг. Зөөврийн болоод суурин компьютер, гар утас, PDA (Personal Digital Assistant) гэх мэт тухайн байгууллагын сүлжээнд холбогдож байсан төхөөрөмжүүд энэ төрлийн халдлагын бай болох боломжтой. Иймд эдгээр төхөөрөмжүүдийн аюулгүй байдал тэдгээрийн виртуал сүлжээнд хандах холболтын аюулгүй байдлыг хангах нь халдлагаас сэргийлэх томоохон арга хэмжээнүүдийн нэг.

Виртуал аюулгүй байдал

Аюулгүй байдлын хувьд яригдах дараагийн асуудал бол зайнаас виртуал сүлжээнд зөвшөөрөлгүй хандах хандалтаас сэргийлэх юм. Физик төрлийн аюул заналаас гадна сүлжээний администратор санаа зовох асуудлын нэг бол яахын аргагүй виртуал аюул заналууд. Ямар нэг утастай холбоонд бол биет байдлаар сүлжээний төхөөрөмж нөөцөд нэвтрэх бол утасгүй сүлжээний хувьд өгөгдлийн урсгал агаараар дамждаг тул зөвшөөрөлгүйгээр нэвтрэх боломж илүү байдаг.

Өгөгдлийн аюулгүй байдал

Өгөгдлийн аюулгүй байдал нь сүлжээгээр дамжиж, боловсруулагдаж, хадгалагдаж буй аливаа өгөгдөл, мэдээллийг хамгаалагдсан байдлыг хамарна. Өгөгдөл нь үйл ажиллагаа явуулж буй байгууллагын хамгийн үнэтэй нөөц бөгөөд түүнд зөвшөөрөлгүй хандах, ямар нэг байдлаар өөрчлөгдөх, дундаас нь барьж аван унших боломжгүй байхаар хамгаалагдсан байх ёстой. Өгөгдөл нь физик сервер дээр байрладаг, тул түүнд физик аюулгүй байдал хэрэгтэй. Мөн өгөгдөл рүү сүлжээнээс хандах боломжтой учир физик болон виртуал аюулгүй байдлын аль аль нь хэрэгтэй. Өгөгдөлд тодорхой хандах эрх хэрэгтэй учир, үүнд өгөгдлийн аюулгүй байдлын нэмэлт хамгаалалт хэрэг болно.

1.1.2 Сүлжээний хамгаалалтын аргууд

Сүлжээ нь мэдээллийн технологийн зайлшгүй чухал систем юм. Компьютерийн систем ба терминалуудын хоорондох бүх харилцаа холбоо нь орон нутгийн (LAN) болон өргөн хүрээний сүлжээнд (WAN) явагддаг. Өдөр бүр янз бүрийн мэдээлэл, нөөцийг солилцдог. Сүлжээний

тусдаа зангилаа нь кабел, радио холболт, залгах эсвэл түрээслэх шугамаар хоорондоо холбогддог. Яг эдгээрт тусгай хамгаалалт шаарддаг. Сүлжээний хамгаалалт гэдэг нь сүлжээ болон таны өгөгдлийг удирдахаас хамгаалах аливаа үйл ажиллагааг хэлнэ. Үүнд техник хангамж, програм хангамжийн технологи, аюулгүй байдлын холбогдох стратегиуд орно. Энэ нь юуны түрүүнд сүлжээнд нэвтэрч тархахаас, дараа нь сүлжээнд гэмтэл учруулахаас урьдчилан сэргийлэх явдал юм. Сүлжээний хамгаалалтын хэд хэдэн төрлийг энд дурдах болно:

- Antivirus software / Вирусны эсрэг програм хангамж
- Application security / Хэрэглээний аюулгүй байдал
- Behavioral analysis / Зан төлөвийн шинжилгээ
- Avoidance of data loss / Мэдээлэл алдахаас зайлсхийх
- Firewalls (web application firewalls) / Галт хана (вэб програмын галт хана)
- VPN / Виртуал хувийн сүлжээ
- Browser/Web Security / Хөтөч / Вэб аюулгүй байдал

Хандалтын хяналт - Access control

Хандалтын хяналт нь хэрэглэгчийн үүрэг хариуцлагатай шууд хамааралтай бөгөөд сүлжээний нөөцийг хязгаарлах замаар сүлжээний хамгаалалтаа нэмэгдүүлэх боломжийг олгодог.

Хортой програмаас хамгаалах програм - Anti-malware software

Вирус, троян, өт, keylogger, spyware гэх мэт хортой програм нь компьютерийн системээр дамжин тархаж, сүлжээнд халдварлах зориулалттай. Хортой програмын эсрэг хэрэгсэл нь аюултай програмуудыг таних, тархахаас урьдчилан сэргийлэхэд зориулагдсан сүлжээний аюулгүй байдлын програм хангамжийн төрөл юм. Вирусийн эсрэг програм нь сүлжээнд учирч болзошгүй хохирлыг багасгах боломжтой юм.

Гажиг илрүүлэх - Anomaly detection

Сүлжээний гажиг илрүүлэх хөдөлгүүрүүд (ADE) нь сүлжээгээ шинжлэх боломжийг олгодог бөгөөд ингэснээр зөрчил гарсан тохиолдолд танд хариу өгөх чадвартай хангалттай хурдан анхааруулах болно.

Хэрэглээний аюулгүй байдал - Application security

Олон халдагчдын хувьд програмууд нь ашиглах боломжтой хамгаалалтын эмзэг байдал юм. Аппликэшны аюулгүй байдал нь таны сүлжээний аюулгүй байдалд хамааралтай бүх програмын аюулгүй байдлын параметрүүдийг бий болгоход тусалдаг.

Мэдээлэл алдахаас урьдчилан сэргийлэх (DLP) - Data loss prevention

Ихэнхдээ сүлжээний аюулгүй байдлын хамгийн сул холбоос бол хүний элемент юм. DLP технологи ба бодлого нь ажилтнууд болон бусад хэрэглэгчдийг эмзэг өгөгдлийг буруугаар ашиглахаас урьдчилан сэргийлэх, сүлжээнд холбогдох өгөгдөл оруулахаас хамгаалахад тусалдаг.

Мэйлийн аюулгүй байдал - Email security

DLP-тэй адил э-мэйлийн аюулгүй байдал нь хүнтэй холбоотой аюулгүй байдлын сул талыг арилгахад чиглэгддэг. Фишинг стратеги ашиглан (ихэвчлэн маш төвөгтэй бөгөөд үнэмшилтэй байдаг) халдагчид э-мэйл хүлээн авагчдыг ширээний эсвэл хөдөлгөөнт төхөөрөмжөөр дамжуулан нууц мэдээллийг хуваалцахыг ятгаж, зорилтот сүлжээнд

санамсаргүйгээр хортой програм татаж авахыг ятгадаг. Э-мэйлийн аюулгүй байдал нь аюултай э-мэйлийг танихад тусалдаг бөгөөд халдлагыг хааж, чухал өгөгдөл хуваалцахаас хамгаалахад ашиглаж болно.

Төгсгөлийн цэгийн аюулгүй байдал - Endpoint security

Бизнесийн ертөнц таны хувийн төхөөрөмжийг (BYOD – Bring Your Own Device) улам бүр нэмэгдүүлж, хувийн болон бизнесийн компьютерийн төхөөрөмжүүдийн хоорондын ялгаа бараг байхгүй болж байна. Төгсгөлийн цэгийн аюулгүй байдал нь алсын төхөөрөмжүүд болон бизнесийн сүлжээнүүдийн хоорондох хамгаалалтын давхаргыг нэмж өгдөг.

Галт хана - Firewall

Галт хана нь таны сүлжээ болон интернетийн хоорондох хил хязгаарыг хамгаалахад ашиглаж болох хаалга шиг ажилладаг. Галт хана нь сүлжээний урсгалыг удирдахад ашиглагддаг бөгөөд зөвшөөрөлгүй траффикийг хааж , зөвшөөрөлтэй траффикийг дамжуулдаг.

Халдлагаас урьдчилан сэргийлэх систем - Intrusion prevention systems

Халдлагаас урьдчилан сэргийлэх систем (халдлагыг илрүүлэх) сүлжээний траффик / пакетуудыг байнга сканердаж, дүн шинжилгээ хийдэг бөгөөд ингэснээр өөр өөр төрлийн халдлагыг олж илрүүлж, хариу арга хэмжээ авах боломжтой болно. Эдгээр системүүд нь аюул заналыг даруй таних чадвартай байхын тулд мэдэгдэж буй халдлагын аргуудын мэдээллийн санг ихэвчлэн хадгалдаг.

Сүлжээний сегмент - Network segmentation

Аюулгүй байдлын өөр өөр эрсдэлтэй холбоотой олон төрлийн сүлжээний урсгал байдаг. Сүлжээний сегмент нь сэжигтэй эх үүсвэрээс гарах урсгалыг хязгаарлахын зэрэгцээ зөв траффикт, зөв хандалтыг өгөх боломжийг олгодог.

Аюулгүй байдлын мэдээлэл ба үйл явдлын менежмент (SIEM) - Security information and event management (SIEM)

Заримдаа олон янзын хэрэгслээр дамжуулан зөв мэдээллийг авах нь туйлын хэцүү байдаг. SIEM багаж хэрэгсэл нь хүмүүст ажиллахад шаардлагатай өгөгдлийг хурдан шуурхай өгдөг.

Виртуал хувийн сүлжээ (VPN) - Virtual private network (VPN)

VPN хэрэгслийг аюулгүй сүлжээ ба төгсгөлийн цэгийн төхөөрөмжийн хоорондох харилцаа холбоог баталгаажуулах зорилгоор ашигладаг. Алсын хандалттай VPN-үүд нь нэвтрэлтийг баталгаажуулах зорилгоор IPsec эсвэл Secure Sockets Layer (SSL) -ийг ашигладаг бөгөөд бусад талуудыг чагнах боломжийг хаах зорилгоор шифрлэгдсэн шугам үүсгэдэг.

Вэб аюулгүй байдал - Web security

Вэб аюулгүй байдал нь техник хангамжийн бодлого болон бусад зүйлийг багтаасан дотоод сүлжээнд холбогдсон үед вэбийн аюулгүй ашиглалтыг баталгаажуулах зорилгоор сүлжээний аюулгүй байдлын арга хэмжээг тодорхойлдог. Энэ нь сүлжээнд

нэвтрэхийн тулд вэб хөтчийг нэвтрэх цэг болгон ашиглахаас урьдчилан сэргийлэхэд тусалдаг.

Утасгүй аюулгүй байдал - Wireless security

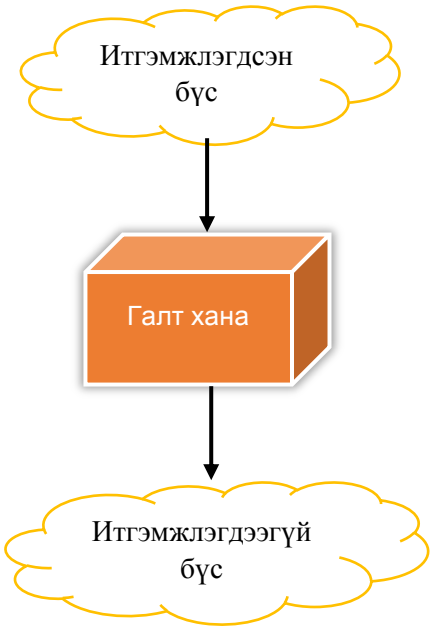
Ерөнхийдөө утасгүй сүлжээ нь уламжлалт сүлжээнээс аюулгүй байдал багатай байдаг.

1.2 Firewall (Галт хана) гэж юу вэ?

Галт хана нь сүлжээний ирж буй болон гарч буй урсгалыг хянах, аюулгүй байдлын тогтоосон багц дүрмийг үндэслэн тодорхой урсгалыг зөвшөөрөх, хориглох эсэхийг шийдэх сүлжээний аюулгүй байдлын төхөөрөмж юм.

Firewall нь дотоод сүлжээ, компьютерийн систем рүү интернет холболтоор дамжин ирж байгаа мэдээллийг шүүх шүүлтүүр бүхий техник хангамжийн төхөөрөмж болон програм хангамжийн цогц хамгаалалтын шийдэл болдог.

Галт хана нь итгэмжлэгдсэн бүс ба итгэмжлэгдээгүй бүсийн хоорондох хөдөлгөөний урсгалыг хянадаг. Эдгээр нь бие даасан бүтээгдэхүүн хэлбэрээр байдаг бөгөөд заримдаа өргөн зурвасын чиглүүлэгчид (рүтер) байдаг. Галт хана нь сүлжээний өөр хэсгүүдэд нэвтрэх боломжийг идэвхгүй болгодог. Ихэнх тохиолдолд эдгээр нь хувийн сүлжээ байна. Галт хананд тодорхой "аюулгүй байдлын дүрмүүд" хэрэгжүүлдэг. Дүрмийг системийн администратор эсвэл компьютерийн эзэмшигч тохируулж болох бөгөөд энэ нь вэб сервер, FTP сервер, telnet сервер гэх мэт серверүүдэд нэвтрэх боломжийг олгодог. Тэд ямар төрлийн холболт хийж болохыг шийддэг байна.



Зураг 1. 1 Firewall төхөөрөмж

1.2.1 Хөгжлийн үе шат

Firewall гэдэг ойлголт 1980-аад оны сүүлчээр гарч ирсэн. Хөгжлийн үе шатыг товч дурдвал:[2]

Нэг дэх үе: Пакет шүүлтүүр (Packet filter)

1988 онд Дижитал Тоног Төхөөрөмжийн Корпорацийн (DEC) Жефф Могул анхны галт хана болох пакет шүүлтүүрийг гаргасан

Хоёр дахь үе: Муж улсын шүүлтүүр (Stateful filter)

1989-1990 оны үед AT&T Bell лабораторид Дэйв Пресетто, Жарнардхан Шарма, Кшитиж Нигам нар хамтран анхны пакет шүүлтүүрийн галт ханын ойлголтыг нэгтгэсэн хоёр дахь үеийн галт хана болох хэлхээний түвшний галт хана боловсруулсан.

Гурав дахь үе: Хэрэглээний түвшний галт хана (Application Layer Firewall)

1990-1991 онд Прудугийн их сургуулийн гений спаффорд AT&T лабораторид Билл Чесвик, Маркус Ранум нар хамтран прокси галт хана дээр суурилсан хэрэглээний түвшний галт хана гэгдэх гуравдах үеийн галт ханыг тодорхойлсон.

Дөрөв дэх үе: Диманик пакет шүүлтүүр (Dynamic Packet Filter)

1991 онд анх хөгжүүлж эхэлсэн боловч гаргаж чадаагүй. 1992 онд USC-ийн Мэдээллийн Шинжлэх Ухааны Хүрээлэнгийн Боб Брэден, Аннетт Дешон нар хамтран "Виза" гэж нэрлэсэн системийн динамик пакет шүүлтүүрийн галт ханыг бие даан судалж эхэлсэн.

Тав дахь үе: Цөмийн прокси галт хана (Kernel Proxy Firewall)

1996 онд “Global Internet Software Group”, Inc-ийн ахлах эрдэмтэн Скотт Вигел цөмийн прокси архитектурыг хөгжүүлж эхэлсэн. Cisco Centri галт ханыг цөмийн прокси архитектур дээр үндэслэн боловсруулж 1997 онд гаргасан.

Зургаа дахь үе: Дараа үеийн галт хана (Next - generation firewall)

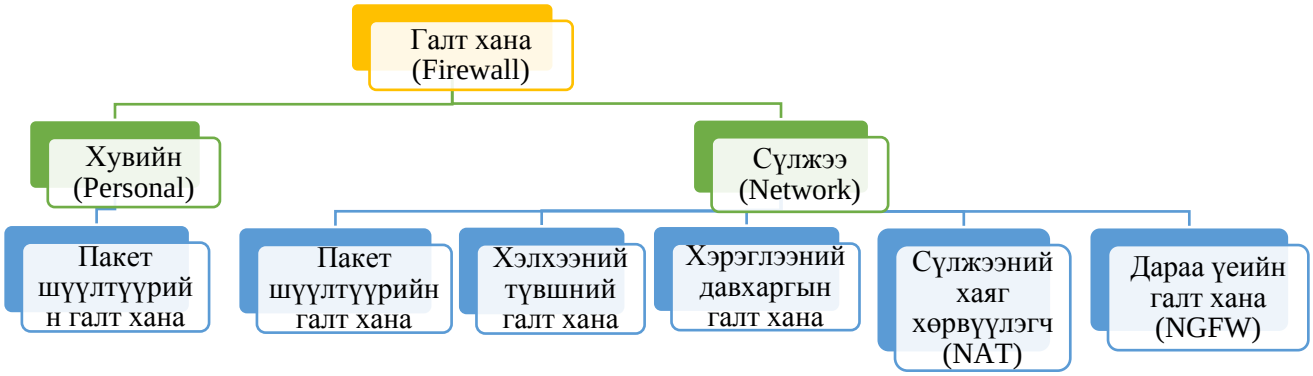
2003 онд Гартнер Next Generation Firewall (NGFW)[3] -ийн санааг судалж эхэлсэн. NGFW нь аюулгүй байдлын шинээр боловсруулсан олон технологийг нэгтгэсэн. Хэрэглээний харагдац ба хяналт, пакетын гүнзгий хяналт шалгалт, аюулаас хамгаалах дэвшилтэт чанар, үйлчилгээний чанар нь NGFW-уудын суурийг бүрдүүлэв. Сүлжээний аюулгүй байдлын асуудлуудыг шийдвэрлэхийн зэрэгцээ NGFW нь администраторуудад компьютерын технологийн үсрэлт, интернетийн өөрчлөгдөж буй орчинтой хөл нийлүүлэн аюулгүй байдлыг хангах боломжийг олгосон.NGFW нь өмнөх галт хананууудын давуу талыг багтаасан бөгөөд гүйцэтгэлийг алдалгүйгээр тагнуул, хяналтыг өргөжүүлж, гүнзгийрүүлж байв. Эдгээр онцлог шинж чанарууд нь пакетуудыг нарийвчлан шалгаж, халдлагад өртсөн эсэхийг тодорхойлох боломжтой.

---

[2] *Docplayer.net. 2020. What Is Firewall? A System Designed To Prevent Unauthorized Access To Or From A Private Network. - PDF Free Download. [online] Available at: <https://docplayer.net/13532423-What-is-firewall-a-system-designed-to-prevent-unauthorized- access-to-or-from-a-private-network.html> [Accessed 22 December 2020].гаргасан*

[3] *Juniper.net. 2020. [online] Available at: <https://www.juniper.net/documentation/en_US/learn-about/LA_FIrewallEvolution.pdf> [Accessed 20 December 2020]. гаргасан*

1.3 Галт ханын ангилал



1.3.1 Архитектурын хувьд

- Техник хангамжийн галт хана
- Програм хангамжийн галт хана

Хүснэгт 1. 1 Техник хангамж ба програм хангамжийн ялгаа

Hardware firewall (Техник хангамжийн галт хана)	**Software firewall (Програм хангамжийн галт хана)**
Техник хангамжийн галт хана нь компьютер болон интернетийн хооронд байрладаг чиглүүлэгч дээр нэгдмэл суусан байдаг.	Програм хангамжийн галт хана нь тус тусын сервер дээр суулгасан байдаг. Холболтын хүсэлт бүрийг таслан зогсоож дараа нь хүсэлтийг хүчин төгөлдөр эсэхийг шалгана.
• Бүх сүлжээг хамгаалдаг • Чиглүүлэгчийн түвшинд хэрэгжүүлдэг • Их үнэтэй • Тохируулахад хэцүү	• Ганц компьютерийг хамгаалдаг • Бага үнэтэй • Тохируулахад хялбар • OS(Operating System) болон Windows 7 үйлдлийн систем дээр нь нэгдсэн галт хана байдаг

1.3.1.1 Техник хангамжийн галт хана (Firewall төхөөрөмж)

Зураг 2. 2 Техник хангамжийн төхөөрөмж

Firewall төхөөрөмж нь таны компьютер болон интернет (эсвэл бусад сүлжээний холболт) хооронд байрладаг. Firewall төхөөрөмж нь компьютерийг хамгаалах, сүлжээний үйл ажиллагааг хянах үүрэгтэй.

Давуу тал	Сул тал
• Компьютерийн системд халдлагаас хамгаалах нэмэлт хамгаалалт болдог.	• Тохиргоо, засвар үйлчилгээгээ дэмжихэд бэлтгэгдсэн мэргэжилтнүүд шаардагдах тусдаа төхөөрөмж юм. Дотоод халдлагад өртөхөд хялбар байдаг.

1.3.1.2 Програм хангамжийн галт хана

Програм хангамжийн галт хана нь компьютер дээр суулгасан програмууд бөгөөд системийг гаднын этгээдийн халдлагаас хамгаалдаг. Системийн оролт, гаралтын урсгалыг хянадаг тул үйлдлийн системийг ачаалалд оруулна.

Давуу тал	Сул тал
• Систем дээрх бие даасан програмуудын сүлжээний ажиллагааг тодорхой түвшинд хянана. • Сүлжээний төгсгөлийн цэгүүдийг бие биеэс нь тусгаарлах замаар илүү сайн хамгаална.	• Сүлжээнд байгаа компьютер бүрд зориулсан галт хана байгаа бол та компьютер бүрийн галт ханыг тус тусад нь шинэчлэх, удирдах шаардлагатай болно. • Гаднын халдлагаас хамгаалах, хортой программуудын эсрэг маш сайн хамгаалалтыг хийдэг ч зөвхөн тухайн програмыг суулгасан тохиолдолд л хамгаална.

1.3.2 Network layer firewall - Сүлжээний түвшний галт хана буюу packet filtering firewalls

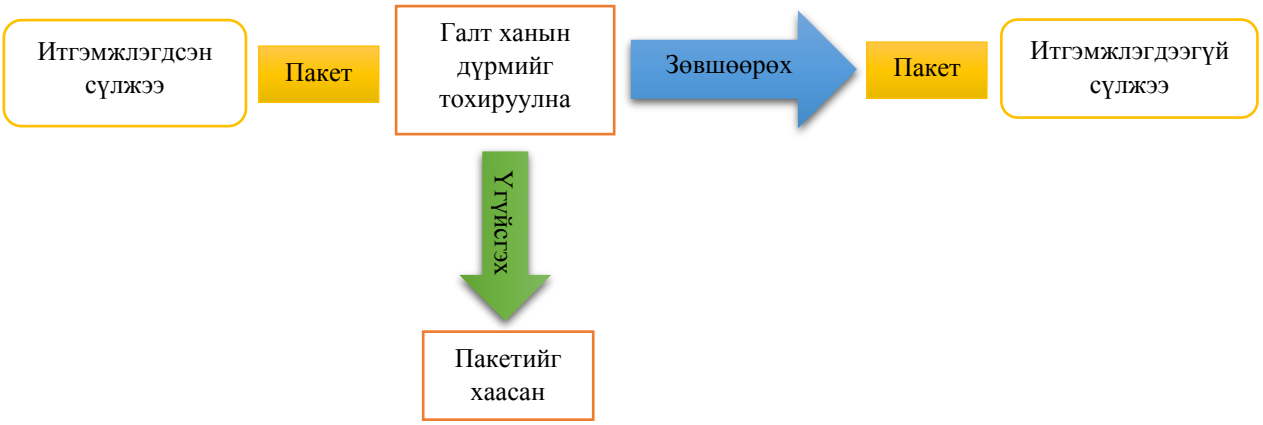
Гүйцэтгэх үүргийн хувьд:

- Packet filtering Stateful (1-р үеийн галт хана)
- Packet filtering Stateless (2-р үеийн галт хана) гэж ангилна.

Stateless	Stateful
Пакет тус бүрийг тусад нь авч үздэг	Муж улсын галт хана нь session талаарх агуулгыг хадгалж, пакет боловсруулалтыг хурдасгахын тулд мэдээллийг ашигладаг
Пакетын толгой дээрх мэдээлэлд үндэслэнэ	Интернет протокол дээр суурилсан
Серверийн хүсэлт нь тус бүрийн мэдээлэлд үндэслэнэ	Хүсэлт нь тус бүрд дамжуулсан мэдээлэл дээр үндэслэнэ
Өмнөх хүсэлт гаргасан мэдээлэлд итгэдэггүй Сервер нь хүсэлтийн мэдээллийг агуулдаггүй	Өмнөх хүсэлт гаргасан мэдээлэл хадгалагдсан байдаг
Өөр өөр серверүүдээс нэг удаа өөр мэдээлэл авах боломжтой	Бүх хүсэлтийг боловсруулахдаа ижил сервер ашиглана

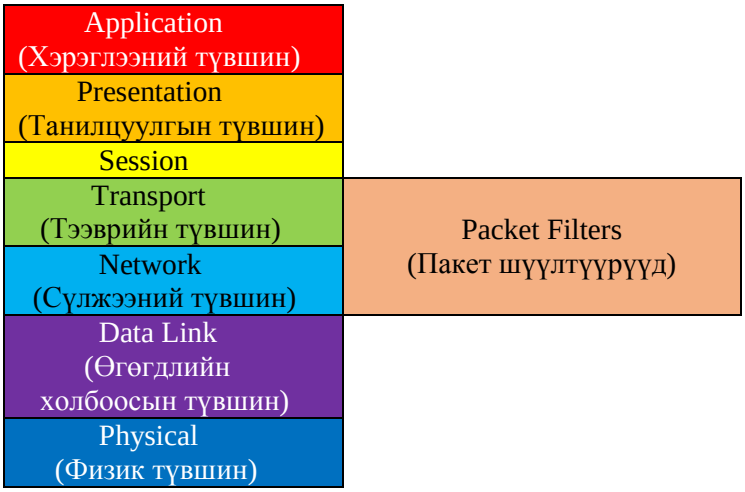
Пакет шүүлтүүрийн галт хана нь пакетуудыг шалгадаг. Пакет шүүлтүүр нь периметрийн аюулгүй байдлын аливаа тохиргоонд ашиг тустай байдаг.

Сүлжээний өгөгдөл гэж нэрлэдэг пакет нь толгой ба өгөгдлийн хэсгээс бүрдэнэ. Пакетын толгой хэсэг нь пакетыг хаах эсвэл галт ханаар дамжуулах эсэхийг шийдэхэд хэрэглэгддэг. Пакет шүүлтүүрийн чиглүүлэгч нь ирж буй болон гарч буй холболтыг шалгаж өгөгдлийн пакетуудыг шүүдэг. Нийтийн сүлжээнд зөвшөөрөлгүй нэвтрэхийг хязгаарладаг. Энэ нь галт хананы дүрмийг зөрчсөн пакетуудыг олж тогтоодог. Пакет шүүлтүүрийн галт хананд тодорхой хязгаарлалтууд байдаг. Тэд мөн хаягийн хязгаарлалтыг хэрэгжүүлдэг.



Давуу тал	Сул тал
• Пакетийг боловсруулахад шаардагдах хугацаа хурдан байдаг. • Пакет шүүлтүүрийг хялбархан хэрэгжүүлж болно. • Пакет шүүлтүүрийн галт хана нь бага өртөгтэй. • Пакет шүүлтүүрийн галт хана нь програмаас хамааралгүй байдаг. Шийдвэр гаргахдаа програмын мэдээлэлд бус харин пакетийн толгой хэсэгт байгаа мэдээлэлд үндэслэнэ.	• Пакет шүүлтүүрүүд нь өгөгдөлд өртөх эрсдэлд хүргэж болзошгүй. • Пакет шүүлтүүр нь уян хатан чанарыг санал болгодог. • Дүрмийг тодорхойлох нь нарийн түвэгтэй. • Пакет шүүлтүүрийн галт хана нь хэрэглэгчийн баталгаажуулалтыг гүйцэтгэдэггүй.

Пакет шүүлтүүр нь үндсэндээ сүлжээний түвшин дээр ажилладаг.



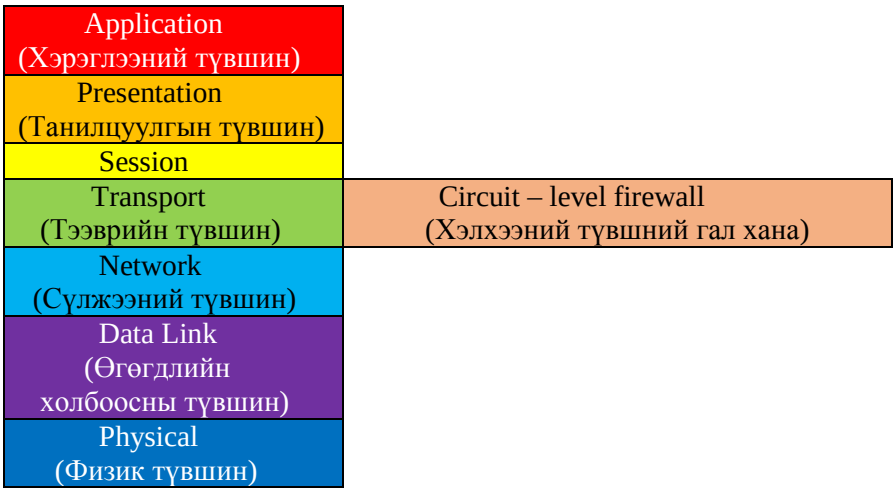
1.3.3 Circuit - level firewall – Хэлхээний түвшний галт хана

Хэлхээний түвшний галт хана нь хувийн пакетуудыг шалгадаггүй. Энэ нь TCP[4] эсвэл UDP[5] session хянадаг. Session байгуулагдсаны дараа тухайн session-д хамаарах бүх пакетуудыг нэвтрүүлэх үүднээс портыг нээлттэй орхино. Session дуусгавар болоход порт хаагдана. Өгөгдөл солилцох боломжийг олгохоос өмнө холболтыг баталгаажуулдаг. Энэ нь дүрмийн дагуу пакетуудыг зөвшөөрөх эсвэл зөвшөөрдөггүй мөн түүнчлэн төгсгөлийн холболт хүчин төгөлдөр эсэхийг тодорхойлдог. Энэ нь хязгаарлагдмал хугацаанд зөвхөн зөвшөөрөгдсөн эх үүсвэрийн пакетуудын хөдөлгөөнийг зөвшөөрдөг. Мэдээлэл солилцох session бүрийг баталгаажуулж, хянах бөгөөд хэрэв session нээгдээгүй бол бүх траффикийг хориглоно.

Холболтын баталгаажуулалтыг дараах зүйл дээр үндэслэн хийнэ.

- Очих IP хаяг эсвэл порт
- Эх үүсвэрийн IP хаяг эсвэл порт
- Протокол
- Хэрэглэгч

Хэлхээний түвшний галт хана нь OSI загварын тээврийн түвшин дээр ажилладаг.



1.3.4 Application layer firewall – Хэрэглээний түвшний галт хана (3-р үеийн)

- Network based Сүлжээнд суурилсан галт хана
- Host based Хост-д суурилсан галт хана
- Next generation Дараа үеийн галт хана (2012)

Энэ нь ихэвчлэн хоёр сүлжээний интерфейсээр тохируулсан аюулгүй хост систем дээр хэрэгждэг. Хэрэглээний түвшний галт хана нь хоёр төгсгөлийн цэгүүдийн хооронд зуучлагчийн үүрэг гүйцэтгэдэг. Төгсгөлийн цэг бүр нь зөвхөн гарцаар дамжин өөр хоорондоо харилцах боломжтой. Найдваргүй сүлжээнээс үйлчлүүлэгч хүсэлт явуулахад зөвшөөрөгдсөн програмын гарцтай холболт үүсдэг. Прокси нь хүсэлтийг дүрмийн дагуу хүчинтэй эсэхийг тодорхойлдог. Дараа нь үйлчлүүлэгчийн өмнөөс очих газар руу шинэ хүсэлт илгээнэ. Хүсэлтийг хүчинтэй эсэхийг тогтоохын тулд буцааж илгээдэг. Дараа нь үүнийг үйлчлүүлэгч рүү илгээнэ.

[4] Transmission Control Protocol
[5] User Datagram Protocol

Хоёр холболт шаардлагатай:

1. Эх үүсвэрээс гарц руу
2. Нөгөө нь гарцаас очих газар руу.

Application (Хэрэглээний түвшин)	Application layer firewall (Хэрэглээний түвшний галт хана)
Presentation (Танилцуулгын түвшин)	
Session	
Transport (Тээврийн түвшин)	
Network (Сүлжээний түвшин)	
Data Link (Өгөгдлийн холбоосны түвшин)	
Physical (Физик түвшин)	

Энэ нь OSI загварын хэрэглээний түвшинд ажилладаг.

Давуу тал	Сул тал
• Аюулгүй байдлыг дээд зэргээр хангаж өгдөг. • Хэрэглээний түвшний бүрэн дүүрэн мэдээллээр хангадаг. • Төгсгөлийн цэгүүдийн хооронд шууд холболт хийхийг зөвшөөрдөггүй. • Тэд галт ханаар дамжин өнгөрөх хөдөлгөөнд илүү хяналт тавьж ажилладаг. • Агуулгыг хамгийн сайн шүүх чадвартай.	• Тохируулга хийхэд маш түвэгтэй • Хэрэглээний гарц удаан • Бага уян хатан.

1.3.5 Network Address Translation (NAT) – Сүлжээний хаяг хөрвүүлэгч

Галт хананууд нь сүлжээний хаяг хөрвүүлэгч (NAT) ашиглаж олон хаяг руу хөрвүүлэх замаар галт ханаар хамгаалагдсан сүлжээг бүрэн нуудаг. Ихэнх сүлжээний хаяг хөрвүүлэгч (NAT) нь бүх сүлжээнд ашигладаг нэг нийтийн IP хаяг байдаг. Сүлжээнээс гадуур гарах бүх пакетууд аюулгүй байдлын үүднээс дотоод IP хаягуудаа нуусан байдаг тул ирж буй пакетуудыг сүлжээний нийтийн IP хаягаар хүргэж өгдөг. NAT галт хана нь хувийн сүлжээнд байгаа төхөөрөмж хүсэлт гаргасан тохиолдолд л интернетийн траффикийг гарцаар нэвтрүүлэх замаар ажилладаг. Аливаа хүсээгүй хүсэлт эсвэл өгөгдлийн багцыг хаяж, интернетэд аюултай төхөөрөмжүүдтэй холбогдохоос сэргийлдэг. Сүлжээний хаяг хөрвүүлэгчийн (NAT) галт хана нь сүлжээг танихаас хамгаалдаг бөгөөд дотоод IP хаягийг интернетэд харуулдаггүй. NAT-ийн сул тал бол IP хаягийн мэдээллийг агуулсан протоколуудыг пакетын өгөгдлийн хэсэгт зөв дамжуулж чадахгүй.

1.3.6 Next – generation firewall (NGEW) – Дараа үеийн галт хана

Дараа үеийн галт хананы (NGFW) шийдэл нь порт болон протоколын бүх түвшинд **Intrusion Prevention Inspection** буюу халдлагын урьдчилсан хамгаалалт**, Blocking to add application-level** буюу апплейкэйшн түвшний халдлагын эсрэг хамгаалалт хийдэг шинж чанартай байхаар тодорхойлогдсон байдаг. Үндсэн шийдэл нь төхөөрөмж болон хиймэл оюун ухаанд суурилсан програм хангамжтай хослон ажиллах болсон. Энгийн галт хана нь 1-4 давхарга хүртэл хамгаалж чаддаг бол дараа үеийн сүлжээний галт хана нь 7 давхарга хүртэл бүрэн хамгаалдгаараа давуу талтай. Дараа үеийн галт хана (NGFW) нь байгууллагыг дотоод болон гадаад аюулаас хамгаалах зорилгоор сүлжээний урсгалыг шүүж өгдөг. Пакет шүүлтүүр, IPsec болон SSL, VPN дэмжлэг, сүлжээний хяналт, IP зураглалын онцлог зэрэг муж улсын галт хананууудын онцлог шинж чанарыг хадгалахын зэрэгцээ NGFW нь агуулгыг шалгах гүнзгий чадварыг эзэмшдэг. Эдгээр чадварууд нь халдлага, хортой програм болон бусад аюулыг таних боломжийг олгож дараагийн үеийн галт хана (NGFW) нь аюулыг хаах боломжийг олгодог.[6]

1.4 FortiNet

Хамгаалалтын хамгийн шилдэг шийдэл хэмээх нэрийг байнга хадгалж яваа **FortiNet** компанийн бүтээгдэхүүн **FortiGate** галт хана нь **NGFW** үйлдвэрлэгч хөгжүүлэгч салбартаа тэргүүлдэг ба **FortiGate** төхөөрөмжид өөрийн зохион бүтээсэн SOC CPU-г суурилуулан илүү хурдтай, илүү найдвартай олон төрлийн халдлага руу чиглэсэн хамгаалалтыг цогцлоосон.

ASIC буюу **Application specific Integrated Circuit** нь нэгэн зэрэг олон үйлдлийг өндөр хурдаар гүйцэтгэх чадамж бүхий технологи юм.

FortiASIC нь зөвхөн **Fortigate**-ийн моделиудад зориулан гаргасан ба ихэнх моделиудад суулгаж өгснөөр **CPU** дээрх ачааллыг бууруулах бөгөөд **throughput performance**-ийг хамгийн хурдтай байлгахаар бүтээгджээ.

Fortigate төхөөрөмжийн хувьд байгууллагын цар хүрээнээс хамаараад 25mbps-80gbps хүртэлх хүчин чадалтай юм.

Энэ бол жижиг, дунд болон томоохон аж ахуйн түвшний байгууллагад зориулсан Firewall, IPsec болон SSL VPN, Application Control, Intrusion Prevention, Anti-Malware, AntiSpam, P2P Security, Web Filtering хийдэг аюулгүй байдлын цогц шийдэл юм.

1.4.1 FortiGate Firewall-ийн онцлогууд

1. NAT/Route горим болон Transparent горимоос сонгон суурилуулах боломжтой. **NAT/Route** горим нь энгийн тохиргоо бөгөөд **Transparent** горимоор суурилуулахад IP хаягийн тохиргоо шаардлагагүй ба дотоод сүлжээний зохион байгуулалтыг өөрчлөх цаг хугацаа хэмнэсэн амар суурилуулалт юм.

[6] *Itzone.mn. 2020. ITZONE - Дараа Үеийн Аюулгүй Байдлын Нэр Томьёоны Тайлбар. [online] Available at: <https://www.itzone.mn/content/blog/show/53> [Accessed 30 November 2020].*

2. **Antivirus - FortiGate** төхөөрөмж нь вирусээс хамгаалах боломжтой. Бүхий л төрлийн халдлагыг судалдаг **FortiGuard**-с 24 цагийн турш автоматаар хамгийн сүүлийн үед судлагдсан халдагын мэдээллийг илгээж хамгаалдаг байна.

3. **WebFiltering -** Интернетээр дамжин phishing site,malware,virus бүхий вэб хуудас руу автоматаар шилжих түүн рүү хэрэглэгч өөрөө нэвтрэхээс сэргийлсэн технологи юм. Ямар нэг байдлаар хортой вирус бүхий сайтууд руу нэг хэрэглэгч л нэвтрэхэд дотоод сүлжээнд аюул учруулж чаддаг. Вэб сайт-д байршсан хортой кодуудыг танин автоматаар блок хийж чаддаг байна. **Fortinet** компаниас гаргасан 4,700,000 сайтаас URL кодыг танин дээрх сайтуудыг энгийн сайтаас ялгаж чаддаг.

4. **Antispam -** Байгууллагын үүд хаалга болсон и-мэйлээр дамжин халдлага орж ирэх өндөр магадлалтай байдаг. Spam мэйл-нд хууртан түүн доторх хортой файлыг нээх татаж авах зэргээр дотоод сүлжээнд нэвтэрдэг. **FortiGuard** нь өндөр зэрэглэлийн anti-spam нэвтрүүлэн, давхар шүүлтүүр ашигладгаараа бусад галт хананаас ялгаатай байгаа юм. Virus Bulletin-аас гаргасан 2015 оны **VBSPAM** тестээр 99.98% амжилттай туршигдсан.

5. **Application control -** Энэхүү feature нь хэрэглэгчийн хэрэглэж буй application-ийг real time-ээр хянаж тэдгээрийг хязгаарлах боломжтой. **FortiGuard application control**-ийг ашиглан тус бүрд нь болон багцалж хязгаарлаж чадна. Жишээлбэл: Байгууллагын нэг хэрэглэгч ажил дээрээ олон нийтийн сүлжээгээр зочлох, тоглоом татаж авах зэргээр ажлын бүтээмж бууруулах , дотоод сүлжээнд аюул бүхий үйлдэл хийж байгааг хянаж хаалт хийхийг хэлж байгаа юм.

6. **IPS -** Уламжлалт галт ханын нэг онцлог болох **IDS /Intrusion detection systems/** нь халдлага илэрсэн тохиолдол түүнийг мэдээлдэг ба тухайн халдлагыг зогсоохын тулд гар ажиллагаа болон цаг хугацаа шаарддаг байсан. **IPS /Intrusion Prevention systems/** халдлагыг илрүүлсэн тохиолдол шууд зогсоож чаддаг болсноороо цаг алдахгүй найдвартай хамгаалдаг болсон.

7. **VPN / Virtual Private network/ - Fortigate VPN throughout** хурд нь үүнийг тодорхой харуулах ба энэ нь ажил дээрээ байхгүй байсан ч зайнаас компанийн дотоод сүлжээ рүү VPN ашиглан нэвтрэх боломжийг хэлнэ.**VPN throughput** хурд өндөр байх тусмаа хэдэн ч хүн зайнаас хандахад сүлжээ гацахгүй байна. Дижитал шилжилтийг уриа болгосон өнөө үед интернетийн сүлжээ байгаа тохиолдолд хаанаас ч ажлаа явуулах нь байгууллага болоод ажилчдад хамгийн хэрэгтэй.

8. **SSL inspection -** Нэг хэрэглэгчээс сервер лүү хандах тохиолдолд замд нь мэдээллийг кодолж нууцлах ба яг энэ үед **UTM / Unified threat management/** ажиллан мэдээллийг дахин задалж үзээд сервер лүү хандахад бэлэн болгох бөгөөд мэдээллийг цааш дамжуулахдаа дахиж кодлон нууцалсан файл болгон илгээнэ.

9. **VDOM / Virtual Domain /** - Нэг галт хана төхөөрөмжийг дотор нь хуваан хэд хэдэн төхөөрөмж болгох боломжтой. Жишээлбэл: Нэг барилга дотор тусдаа хэд хэдэн компаниуд эсвэл салбар хэлтсүүд байрладаг гэж үзэхэд эдгээр компаниуд нь тус тусдаа галт хана төхөөрөмж хэрэгтэй байх үед нэг төхөөрөмжийг дотор нь virtual domain буюу VDom хэлбэрээр хуваан тус бүрд нь тохиргоо хийж болохуйц виртуал төхөөрөмжүүдийг ашиглах боломжтой.

10. **Virtual machine - Fortigate** галт ханыг виртуал хэлбэрээр ашиглах боломжтой ба тухайн байгууллагын сервер дээр суурилуулан физик төхөөрөмжөөс ямар ч ялгаагүй, тохиргоо болон хэрэглээний хувьд яг адилхан байдлаар хэрэглэж болох юм.

Олон төрлийн халдлагаас хамгаалах дээрх технологийг нэг төхөөрөмжид багтаасан ба дэлхийн хамгийн хурдан шүүх чадамжтай галт хана хэмээгддэг **FortiGate** нь дотоод сүлжээн дэх эрсдэл өндөртэй хэрэглэгчийг илрүүлэх мөн цаашлаад удирдлагууд болон холбогдох ажилчдад давуу эрх олгох, интернетийн хурдны удаашралтай байгаа шалтгааныг олох гэх мэт дотоод сүлжээг зохион байгуулах тохиргоо хийх боломжоор дүүрэн байдаг байна.Сүлжээний хамгаалалтыг нэгдсэн нэг удирдлагаар хангах,ойлгомжтой тайлангууд гарган үзүүлэх зэрэг дан ганц хамгаалах үүргээс гадна олон нөөц бололцоог бүрдүүлдэг.

Давуу талууд: Байгууллагын хэрэглэгч бүрийн интернет хандалтыг зохион байгуулж, шаардлагатай эрх бүхий хүмүүс нэвтрэх боломжтой сүлжээг зохион байгуулах Wed filtering хийдэг. Мөн удирдлагуудад зориулсан давуу эрх олгох, хурдны хязгааргүй хэрэглээг нэвтрүүлэх боломжтой. Энэ мэтчилэн интернет орчинд нэвтрэхэд гаднаас ирж болзошгүй халдлагуудаас сэргийлж, таны аюулгүй байдлыг хангах болно.

1.4.2 FortiMail

FortiMail нь хэрэглэгч байгууллагуудад цахим шуудангийн аюулгүй байдлыг хангахад зориулсан шийдэл юм. Энэ нь гаднаас ирэх халдлага болон Malware-уудаас хамгаалах мөн гадагшаа өгөгдлийг алдагдахгүй байх боломжуудыг олгоно.

FortiMail шийдлийн давуу талууд:

- Өндөр түвшний Anti-Spam, Anti-Phishing технологи - Цахим шуудангийн халдлагын гол төрөл болох SPAM болон хуурамч и-мэйлийг илрүүлэх, халдлагаас хамгаалах технологитой.
- Итгэмжлэгдсэн хамгаалалтын шийдэл - Ransomware халдлага, хортой код, өгөгдлийн хулгай, залилан зэргээс аюулаас бүрэн хамгаалдаг.
- Өгөгдөл хамгаалалт - Олон улсын өгөгдөл хамгаалах дүрэм, журам болон байгууллагын журам, зохицуулалттай уялдан ажиллах боломж бүхий өгөгдөл хамгаалалтын технологитой.
- Байгууллагын и-мэйл орчны хяналт, удирдлага - Байгууллагын и-мэйл орчны хяналт, аюулгүй байдлыг бүрэн хянах, удирдах, зохицуулах боломжтой.

Fortinet Fortimail : Secure Email Gateway боломжууд

Fortiguard AntiSpam Service

Байгууллагын тань и-мэйл орчны аюулгүй байдал, тэр дундаа SPAM буюу хэрэгцээгүй хуурамч и-мэйлээс бүрэн сэргийлэг боломжийг олгоно. Fortiguard Labs нь өдөр бүр минутад 21000 орчим SPAM и-мэйл блок хийдэг бөгөөд 46 сая шинэ болон шинэчлэгдсэн SPAM-н дүрмийг хүлээн авдаг

- Өндөр түвшний SPAM и-мэйлийн эсрэг хамгаалалт
- Периметр аюулгүй байдал буюу тодорхой орчны аюулгүй байдлыг бүрэн хангах бөгөөд SPAM и-мэйлийг таньснаар дахин ирэх боломжгүй болгоно.
- Өндөр хурдны ажиллагаа болон цаг алдалгүй шинэчлэгддэг/Update/.
- И-мэйлтэй холбоотой үйл ажиллагааны болон удирдлагын зардлуудыг бууруулна
- Байгууллагын дүрэм журамтай нийцэн ажилладаг.

FortiGuard Antivirus Security Service

Malware халдлагаас хамгийн сайн хамгаална. FortiGuard Labs-н тусламжтай олон улсад гарч байгаа шинэ вирус, spyware болон бусад халдлагуудаас бүрэн хамгаална. Тус Lab нь өдөр бүр минут тутам 95,000 орчим malware халдлагуудыг эсэргүүцдэг.

- Олон тооны хяналтын цэгүүдийн тусламжтай өндөр үр дүнтэй халдлагын эсрэг хамгаалалт болон өгөгдөл алдах, гэмтэх эрсдэлийг бууруулна.
- Зардал, өртөг хамгийн бага түвшинд байна.
- Байнгын шинэчлэгддэг сангийн тусламжтай шинэ болон хуучин бүх халдлагуудаас хамгаалах, сэргийлэх боломжийг олгоно.

FortiSandbox Cloud

FortiSandBox Cloud нь клаудад суурилсан аюулгүй байдлын удирдлага хийх боломжтой шийдэл юм.

- FortiSandBox нь олон улсын аюулгүй байдлын лаборатори болох NSS labs, ICSA labs-р итгэмжлэгдсэн халдлагаас хамгаалах технологи юм.
- Ашиглах болон удирдах, хянахад маш хялбар
- Клауд орчинд суурилсан тул та хаанаас ч аюулгүй байдлаа цогц, хялбар хянах боломжтой.
- Fortinet компанийн бусад функцтэй холбогдон ажилладаг.

1.4.3 Fortinet SD-WAN

Fortinet компанийн хувьд **SD-WAN** шийдлийг зах зээлд нийлүүлээд нэлээдгүй хугацаа өнгөрч байна. Өдгөө Дэлхий өнцөг булан бүрд байгаа хэрэглэгчдийн шаардлагад нийцсэн, аюулгүй, төвлөрсөн **orchestration** бүхий бүрэн self-healing **SD-WAN** шийдлийг нийлүүлдэг бөгөөд тус шийдлийн Дэлхийн анхны зориулалтын процессорыг бүтээсэн. Тус компанийн хувьд цаашид **SD-WAN** зах зээлд хамгийн уян хатан, аюулгүй хандах боломжтой **SASE** инновацийг шингээсэн **cloud-delivered** шийдлийг зах зээлд нийлүүлэхээр ажиллаж байна. Учир нь нөхцөл байдалтай холбоотой Дэлхий нийт гэрээсээ ажиллах хэв маяг дэлгэрч байгаатай холбоо клауд шийдлийг ихээхэн сонирхох хандлага нэмэгдсэн. Тиймээс хэрэглэгчид **Fortinet SD-**

WAN шийдлийг **Security-Driven Networking** буюу аюулгүй байдалд суурилсан сүлжээний шийдэл хэмээн сонгодог.

Fortinet SD-WAN шийдлийн хувьд үндсэн 3 үнэ цэнийг хэрэглэгчдэд өгдөг. Үүнд:

- **Business app-aware** буюу өгөгдлийн урсгалын хамгийн эхний пакет дээр байгаа аппликейшнүүдийг ухаалгаар таньж, байгууллагын хэмжээнд хамгийн өргөн ашиглагддаг бизнес аппликейшнүүдийг мэдэх, ажиллагааны хурдыг нь нэмэгдүүлэх боломжийг өгч төлөвлөлт, бодлого, шийдвэр гаргахад тань тусална.
- **Reduce WAN OpEx** буюу WAN-тай холбогдон гарах үйл ажиллагааны зардлыг 40% хүртэл бууруулна.
- **Simplified Operations** буюу WAN сүлжээтэй холбоотой үйл ажиллагааг хялбарчилж, түвэгтэй байдлыг бууруулна.

1.4.4 Fortinet Fabric Management center

Аюулгүй байдлын удирдлагыг **Fortimanager** буюу сүлжээний удирдлагын шийдэл, **FortiAnalyzer** буюу анализ, лог удирдлагын шийдэл зэргийг бүрдэл болох **Fortinet Fabric Management center**-ийг ашиглан биелүүлж чадсан.

Харин NGFW-ийг **Fortimanager**-тай хослуулан ашигласнаар 48 цаг хийдэг байсан шинэчлэлийг 1 цагт л хийдэг болсон байна. Үүний зэрэгцээ **Fortimanager** нь галт ханын удирдлагыг бүрэн автоматжуулах боломжийг олгодог бөгөөд тэд салбарын тоогоо нэмж, галт хана суурилуулах үед ямар нэг тохиргоогүйгээр шууд холбогдох боломжийг олгож байгаа нь асар их зардал, цаг хугацааг хэмнэж байна. Ингэснээр мөн ажилтнаас хамааралтай алдаа ч багасна гэсэн үг юм.

FortiAnalyzer нь тэдэнд компанийн хэмжээнд ашигладаг аюулгүй байдлын шийдлүүдийг нэг талбар дээрээс удирдах, хянах боломжийг олгосон.

Fortinet NGFW төхөөрөмжийн хувьд **Security-Driven** буюу аюулгүй байдлыг бүрэн хангасан сүлжээний шийдлийг байгууллагад олгодог. Мөн үүнээс гадна үндсэн 3 давуу талуудтай.

- **Manage Operational & Security Risks** буюу байгууллагын үйл ажиллагааг тасалдуулалгүйгээр аюул, халдлагаас бүрэн хамгаалах боломжийг олгоно.
- **Reduce Cost & Complexity** буюу бусад төхөөрөмжтэй харьцуулахад суурилуулах болон ашиглахад маш хялбар төхөөрөмж бөгөөд TCO буюу эзэмшлийн зардлыг хамгийн боломжит бага түвшинд байлгана.

- **Improve Operational Efficiency** буюу байгууллагын тань үйл ажиллагаа, цар хүрээ хэр том, өргөн байхаас үл хамааран маш хялбар бөгөөд үр ашигтай ашиглах боломжийг олгоно.

1.4.5 Fortinet үнийн судалгаа

Fortinet 400E		
Model	FG-400E - Fortinet Next general Firewalls -Middle range-400E Series	
Detail	FortiGate-400E, 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated	
Price	USD	MNT
	4,880$	13,588,021.90 ₮

Fortinet 60E		
Model	FG-30E - Fortinet NGFW Entry-level Series FortiGate 30E	
Detail	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports), Max managed FortiAPs (Total / Tunnel) 2 / 2	
Price	USD	MNT
	359$	999,610.63₮

Fortinet 1000D		
Model	FG-1000D - Fortinet NGFW High-end Series FortiGate 1000D	
Detail	Fortinet FG-1000D 2 x 10GE SFP+ slots, 16 x GE SFP Slots, 16 x GE RJ45 ports, 2 x GE RJ45 Management ports, SPU NP6 and CP8 hardware accelerated, 1 x 256GB SSD onboard storage, dual AC power supplies	
Price	USD	MNT
	15,100$	42,044,903.82₮

БҮЛЭГ II. ТУРШИЛТ СУДАЛГААНЫ ХЭСЭГ

2.1 DeMilitarized Zone (DMZ) - Хамгаалалтгүй бүс

DMZ-ийн зорилго нь байгууллагын дотоод сүлжээнд аюулгүй байдлын нэмэлт давхарга нэмэх явдал юм. Байгууллагууд сүлжээний сегментүүдийн аюулгүй байдлын хяналтыг нарийн тохируулах боломжтой. Энэ нь DMZ доторх халдлага илрүүлэх систем (IDS) эсвэл халдлагаас урьдчилан сэргийлэх систем (IPS) –ийг, дамжуулах хяналтын протокол (TCP) порт, Hypertext Transfer Protocol Secure (HTTPS) хүсэлтээс бусад урсгалыг хаахаар тохируулж болно гэсэн үг юм. DMZ сүлжээнүүд нь галт ханануудыг нэвтрүүлснээс хойш гарч ирсэн ба аж ахуйн нэгжийн сүлжээг аюулгүй болгоход гол үүрэг гүйцэтгэдэг. Тэд дотоод сүлжээг халдагчдын бай болохуйц системээс тусад нь хадгалах замаар байгууллагын эмзэг өгөгдөл, систем, нөөцийг хамгаалдаг. DMZ нь байгууллагуудад мэдрэмтгий системд нэвтрэх түвшнийг хянах, багасгах боломжийг олгодог.

Хамгаалалтгүй бүс (DMZ) нь сүлжээний гаднаас нэвтрэх боломжтой хостуудыг дотоод серверүүдээс тусгаарладаг. Хоёр галт ханыг холбосон сүлжээнээс DMZ сүлжээг үүсгэдэг. DMZ нь гаднын сүлжээнээс орж ирж буй траффикийг шүүх аюулгүй байдлын гарцаар хамгаалагдсан байдаг. Үндсэн сүлжээг нэг хост эсвэл дэд сүлжээгээр тусгаарласнаар DMZ-ээр дамжуулан интернет тоглоом, видео хурал, вэб, мэйлийн сервер зэрэг үйлчилгээнд зочилдог хүмүүс таны сервер рүү нэвтрэх эрхгүй болно. DMZ нь вэб сайтад зочлогсдод тодорхой үйлчилгээ авах боломжийг олгодог бөгөөд тэд болон байгууллагын хувийн сүлжээний хооронд буфер үүсгэдэг. DMZ-ээр дамжуулсан өгөгдөл нь тийм ч найдвартай биш тул DMZ-д байрладаг хостууд дотоод сүлжээний бусад үйлчилгээнд нэвтрэх зөвшөөрлийг хатуу хянадаг. Дээрээс нь DMZ доторх хостууд нь гадаад сүлжээг хязгаарлаж, хамгаалагдсан хилийн бүсийг нэмэгдүүлэхэд тусалдаг. Энэ нь хамгаалагдсан сүлжээнд байгаа хостууд дотоод болон гадаад сүлжээтэй харьцах боломжийг олгодог бол галт хана нь DMZ болон дотоод сүлжээний хоорондох бүх траффикийг шалгаж, удирддаг. Гаднын сүлжээнээс холбоо барих талаар хэрэглэгчдэд хүрч болох бүх үйлчилгээг DMZ-д байрлуулж болно. Хамгийн түгээмэл үйлчилгээ нь:

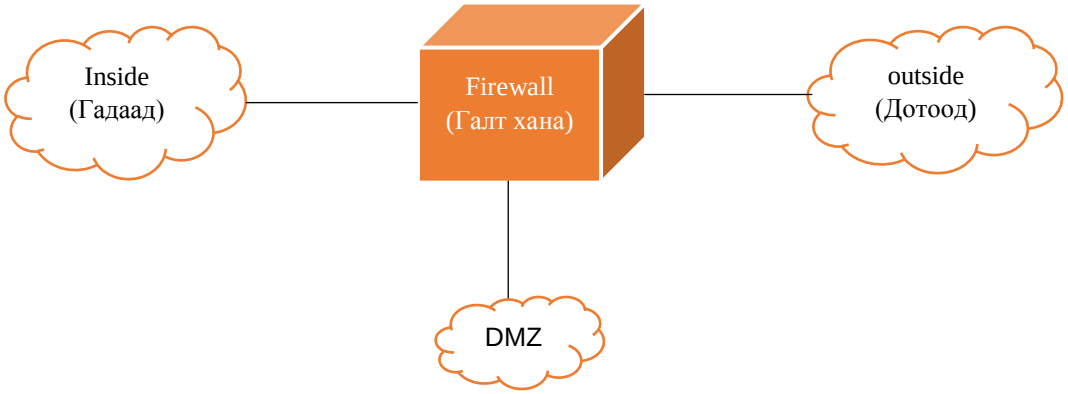
- Вэб серверүүд: Дотоод мэдээллийн баазын сервертэй холбоо барих үүрэгтэй вэб серверүүдийг DMZ дээр байрлуулах шаардлагатай. Энэ нь ихэвчлэн нууц мэдээллийг хадгалдаг дотоод мэдээллийн сангийн аюулгүй байдлыг хангахад тусалдаг.
- Шуудангийн серверүүд: Нэвтрэх эрх, хувийн мессежийг хадгалах зорилгоор бүтээсэн хэрэглэгчийн мэдээллийн сан, ихэвчлэн интернетэд шууд нэвтрэхгүйгээр серверүүд дээр хадгалагддаг. Тиймээс мэйлийн мэдээллийн сантай шууд харьцах, түүнтэй хор хөнөөлтэй траффикт шууд нэвтрэхгүйгээр хандахын тулд мэйлийн серверийг DMZ дотор байрлуулна.
  FTP серверүүд: Эдгээр нь байгууллагын сайт дээр чухал агуулгыг байрлуулж, файлуудтай шууд харьцах боломжийг олгодог. Тиймээс FTP сервер нь чухал дотоод системүүдээс үргэлж хэсэгчлэн тусгаарлагдсан байх ёстой.

2.2 DMZ архитектур

DMZ ашиглан сүлжээ байгуулах олон арга байдаг. Систем бүрийг сүлжээний шаардлагыг хангахуйц нарийн түвэгтэй архитектуруудыг бий болгох зорилгоор өргөжүүлж болно.

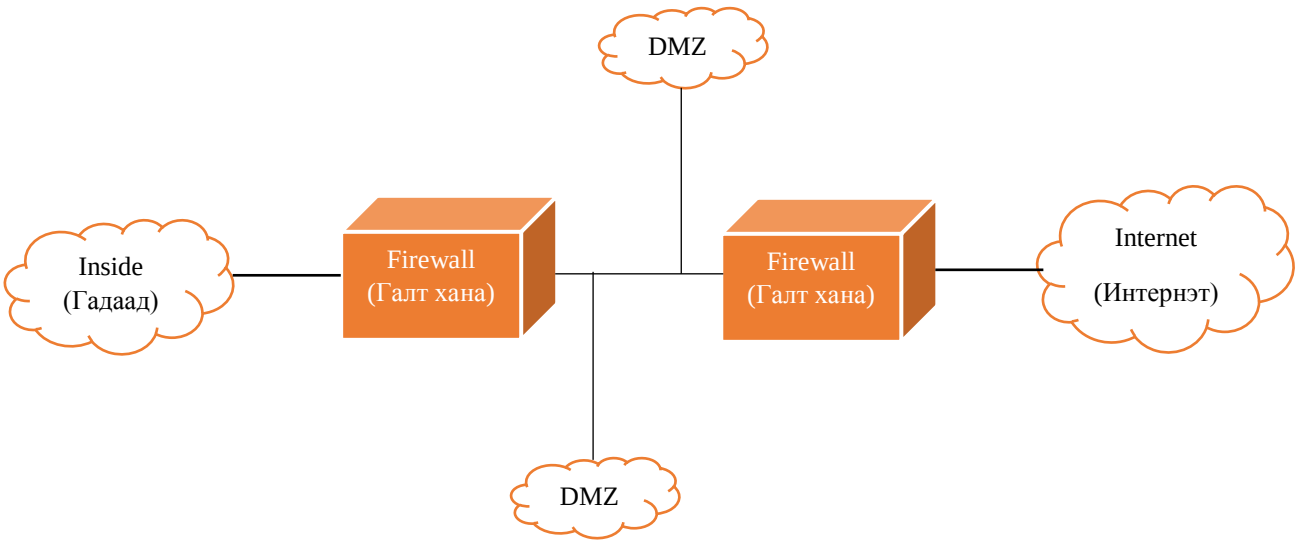
2.2.1 Нэг галт хана (Single firewall)

Сүлжээний архитектурын энгийн арга бол DMZ нь гурван буюу түүнээс дээш сүлжээний интерфейсийг шаарддаг. DMZ-ийг энэ галт хананы дотор байрлуулна. Эхнийх нь нийтийн сүлжээний холболтыг галт хананд холбодог гадаад сүлжээ юм. Хоёр дахь нь дотоод сүлжээг бүрдүүлдэг бол гурав дахь нь DMZ-тэй холбогддог. Төрөл бүрийн дүрмүүд нь DMZ-д нэвтрэх, дотоод сүлжээнд холбогдох хязгаарлалтыг зөвшөөрдөг траффикт хяналт тавьдаг.



2.2.2 Хос галт хана (Dual firewall)

Хос галт ханын хооронд DMZ байрлуулах нь илүү найдвартай арга юм. Эхний галт хана ("урд талын" галт хана гэж нэрлэдэг) нь зөвхөн DMZ-ээс гадаад сүлжээнд зориулагдсан гарах урсгалыг зөвшөөрдөг. Хоёр дахь галт хана ("ард талын" галт хана гэж нэрлэдэг) нь зөвхөн DMZ-ээс дотоод сүлжээ рүү орох урсгалыг зөвшөөрдөг. Байгууллагын LAN сүлжээнд нэвтэрхийн тулд халдагч нь галт хананууудыг хоёуланд нь буулгах шаардлагатай.



2.3 DMZ тохируулах заавар, тайлбар

Хүснэгт 1. 2 DMZ тохируулахад шаардлагатай командуудын тайлбар

Командууд	Тайлбар
User EXEC mode	
Enable	Privileged mode руу хандах
Telnet	Сүлжээгээр хандах
Connect	Terminal-ийн холболтыг нээх
Object network	Объект үүсгэх
Exit	EXEC mode-оос гарах
Help	Тусламж авах
Privileged EXEC mode	
Write memory	Бичсэн тохиргоог хадгалах
Show memory	Санах ойн төлөвийг харах
Show running-config	Одоо ажиллаж байгаа тохиргоог харах
Show startup-config	Эхлэх тохиргоог харах
Show vlan	VLAN-ийн статусыг харах
Show interface ip brief	Интерфейсүүдийн дэлгэрэнгүй мэдээлэл
Show nameif	Интерфейсүүдийн нэрийг харуулна
Show ip address	Интерфейсүүдийн мэдээллүүдийг харуулах
Show switch vlan	Дотор болон гадна талын VLAN-уудыг харуулах
Ping	Холболтыг шалгах
Exit/end	Гарах
Configure terminal	Global conf mode руу хандах
Global configuration mode	
Hostname	Терминалд нэр олгох
Interface	Интерфейсийг сонгож тохиргоо хийх
Enable password	Password олгох
Domain name	Домэйнд нэр олгох
Shutdown	Интерфейсийг унтраах (идэвхгүй болгох)
nameif	VLAN интерфейст нэр олгох
subnet	Дэд сүлжээ үүсгэх
Exit/end	Гарах
IP address [IP] [subnet mask]	IP, Subnet маск

Аюулгүй байдлын түвшин - Security-Level

- **Аюулгүй байдлын доод түвшин - 0** анхдагчаар галт хананы “гадна” интерфейс дээр хуваарилдаг. Аюулгүй байдлын доод түвшин хандалтын жагсаалтад багтаагүй тохиолдолд гаднаас ирж буй траффик аль ч интерфейст хүрч чадахгүй.
- **Аюулгүй байдлын 1-ээс 99-р түвшин** - Аюулгүй байдлын түвшнийг периметрийн аюулгүй байдлын бүсэд хуваарилдаг. Хүссэн хэмжээгээрээ аюулгүй байдлын түвшнийг бий болгож болно. Жишээ: DMZ - ийн аюулгүй байдлын түвшнийг 50 гэж тохируулна. Дотоод сүлжээнээс DMZ (аюулгүй байдлын 100 -> 50), гадна сүлжээнээс DMZ (аюулгүй байдлын 0-> 50) урсгалыг зөвшөөрнө. Гэсэн хэдий ч DMZ - ийн замын хөдөлгөөн дотоод сүлжээ рүү нэвтрэх боломжгүй (хандалтын жагсаалтгүйгээр) аюулгүй байдлын 50-р түвшнээс траффик аюулгүй байдлын 100-р түвшинд хүрэхийг хориглодог.
- **Аюулгүй байдлын дээд түвшин - 100** “дотор” интерфейст хуваарилдаг. Аюулгүй байдлын дээд түвшин тул бүх интерфейсүүдэд хүрч чаддаг.

2.4 Нэг галт ханатай DMZ үүсгэж тохируулсан жишээ

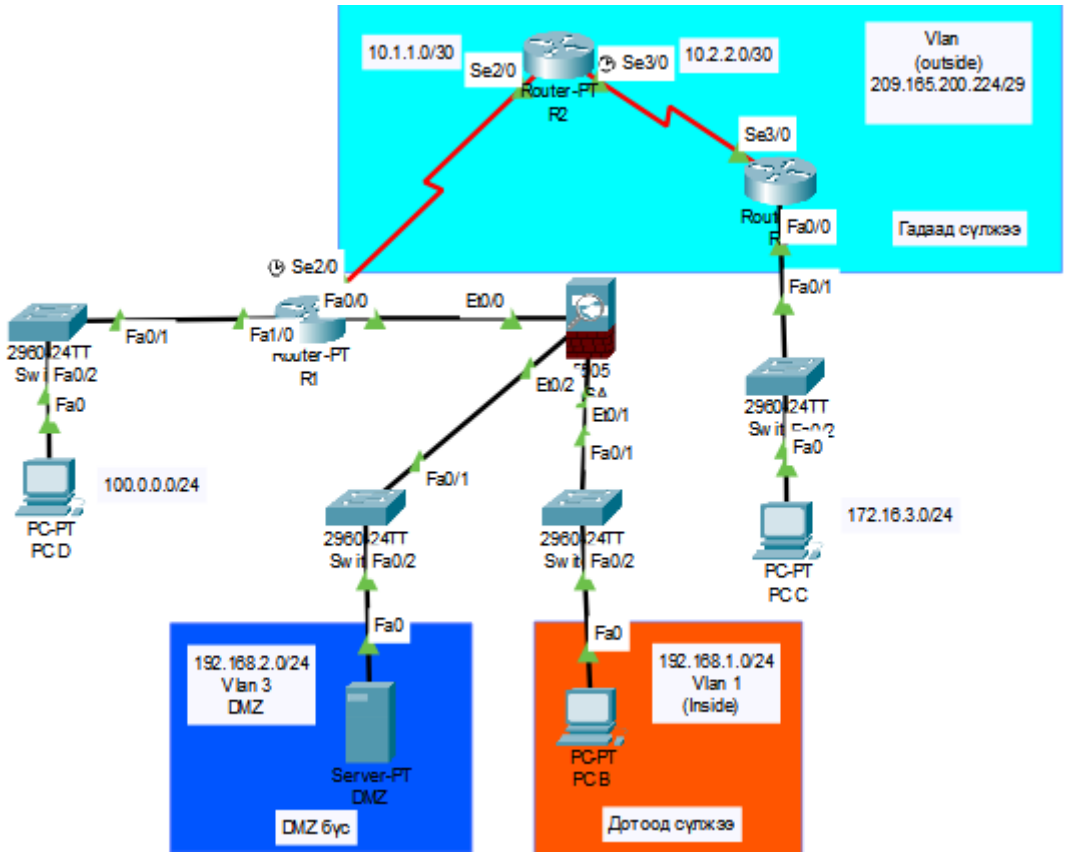
IP хаягийн хүснэгт

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	209.165.200.225	225.225.225.248	N/A
	S2/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S2/0	10.1.1.2	255.255.255.252	N/A
	S3/0 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	Fa0/0	172.16.3.1	255.255.255.0	N/A
	S3/0	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1(Fa0/1)	192.168.1.1	255.255.255.0	N/A
ASA	VLAN 2(Fa0/0)	209.165.200.226	255.255.255.248	N/A
ASA	VLAN 3(Fa0/2)	192.168.2.1	255.255.255.0	N/A
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.3
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1
PC-D	NIC	100.0.0.2	255.255.255.0	100.0.0.1

Тайлбар:

- R1 нь ISP-ийн удирддаг CPE[7] төхөөрөмжийг төлөөлнө.
- R2 нь завсрын интернет чиглүүлэгчийг төлөөлнө.
- R3 нь сүлжээгээ алсаас удирдах сүлжээний менежментийн компанийн администраторыг холбодог ISP юм.
- Layer 3 VLAN интерфейсүүд нь Inside, Outside, DMZ гурван талбарт нэвтрэх боломжийг олгодог.
- ISP нь нийтийн IP хаягийг 209.165.200.224/29-д хуваарилсан бөгөөд үүнийг ASA дээр хаягийн хөрвүүлэлт хийхэд ашиглаж болно.

[7] Харилцаа холбооны тоног төхөөрөмж



Гүйцэтгэх ажил 1: ASA төхөөрөмжийн үндсэн тохиргоо ба интерфейсийн аюулгүй байдлыг тохируулах

Алхам 1: Хостын нэр болон домэйн нэрийг тохируулах

```
ciscoasa>enable  /Privileged горимд шилжиж байна.

ciscoasa# config terminal /Global configuration горимд шилжиж байна.

ciscoasa(config-if)# hostname CCNAS-ASA /Нэрийг CCNAS-ASA болгож
байна.

ciscoasa(config-if)# domain name ccnasecurity.com /Домэйн нэрийг
ccnasecurity.com болгож байна.
```

Алхам 2: Төхөөрөмжид хандах нууц үгийг тохируулах

```
ciscoasa>enable

ciscoasa#config terminal

ciscoasa(config-if)#enable password ciscoenpa55 /нууц үгийг
ciscoenpa55 болгов
```

Алхам 3: Дотор болон гадна талын интерфейсийг тохируулах.

- VLAN 1 (дотор) интерфейсийг тохируулах болно.
- VLAN 2 (гадна) интерфейсийг тохируулах болно.

а. Дотоод сүлжээнд зориулсан логик **VLAN 1** интерфейсийг (192.168.1.0/24) тохируулж аюулгүй байдлын түвшнийг тохируулах дараалал

```
CCNAS-ASA(config)# interface vlan 1 /Интерфейс сонгож байна

CCNAS-ASA(config-if)# nameif inside /Нэр олгох команд

CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0 /IP хаяг
олгож байна

CCNAS-ASA(config-if)# security-level 100 /Аюулгүй байдлын түвшинг
100 гэж тохирууллаа.
```

б. Гадаад сүлжээнд зориулсан логик **VLAN 2** интерфейсийг бий болгож (209.165.200.224/29) аюулгүй байдлын түвшнийг тохируулах дараалал

```
CCNAS-ASA(config-if)# interface vlan 2 / Интерфейс сонгож байна

CCNAS-ASA(config-if)# nameif outside / Нэр олгох команд

CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248

CCNAS-ASA(config-if)# security-level 0
```

Алхам 4: Бүх ASA интерфейсүүдийн статусыг харуулахын тулд **show interface ip brief** командыг ашиглав.

```
ciscoasa(config)#show interface ip brief
Interface              IP-Address      OK? Method Status
Protocol

Ethernet0/0            unassigned      YES unset  up
up

Ethernet0/1            unassigned      YES unset  up
up

Ethernet0/2            unassigned      YES unset  up
up

Ethernet0/3            unassigned      YES unset  down
down

Ethernet0/4            unassigned      YES unset  down
down

Ethernet0/5            unassigned      YES unset  down
down

Ethernet0/6            unassigned      YES unset  down
down

Ethernet0/7            unassigned      YES unset  down
down

Vlan1                  172.16.0.2      YES manual up
up

Vlan2                  200.5.10.1      YES manual up
up

Vlan3                  172.16.1.1      YES manual up
up
```

Show ip address командыг ашиглан VLAN интерфейсүүдийн мэдээллийг харууллаа.

```
CCNAS-ASA(config)#show ip address
System IP Addresses:
Interface              Name                   IP address      Subnet
mask     Method
Vlan1                  inside                 192.168.1.1
255.255.255.0   CONFIG
Vlan2                  outside                209.165.200.226
255.255.255.248 manual
Vlan3                  dmz                    192.168.2.1
255.255.255.0   manual

Current IP Addresses:
Interface              Name                   IP address      Subnet
mask     Method
Vlan1                  inside                 192.168.1.1
255.255.255.0   CONFIG
Vlan2                  outside                209.165.200.226
255.255.255.248 manual
Vlan3                  dmz                    192.168.2.1
255.255.255.0   manual
```

Show switch vlan командыг ашиглан ASA дээр тохируулсан дотор болон гадна талын VLAN-уудыг харууллаа.

```
CCNAS-ASA(config)#show switch vlan

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    inside                           up        Et0/1, Et0/3, Et0/4,
Et0/5
                                                Et0/6, Et0/7
2    outside                          up        Et0/0
3    dmz                              up        Et0/2
```

Алхам 5: ASA холболтыг шалгах.

а. Хэрэв холболт хэвийн бол PC-B-ээс ASA интерфейсийн хаяг руу **ping** хийх боломжтой байх ёстой (192.168.1.1).

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

б. PC-B-ээс VLAN 2 (гадна) интерфейс рүү IP хаягаар (209.165.200.226) нь ping хийж харуулав. Энэ хаягийг пинг хийх боломжгүй байх ёстой. Яагаад гэвэл холбогдох IP

хаягийг **ping** хийх үед өгөгдлийг дамжуулж хариу авах “хүсэлтийн хугацаа дууссан” алдаа гарч байна.

```
C:\>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Гүйцэтгэх ажил 2: CLI ашиглан рүтер дээр хаягийн хөрвүүлэлтийг тохируулах.

Алхам 1: ASA-ийн статик анхдагч чиглүүлэлтийг тохируулах.

ASA-г гаднын сүлжээнд нэвтрэх боломжийг олгохын тулд ASA-ийн гаднах интерфейс дээр анхдагч статик чиглүүлэлтийг тохируулах дараалал.

а. Чиглүүлэлтийн командыг ашиглан "quad zero" анхдагч чиглүүлэлтийг үүсгээд ASA гадна интерфэйстэй холбож, R1 fa0/0 IP хаягийг (209.165.200.225) хамгийн сүүлчийн гарц болгон зааж өгнө.

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

б. Статик анхдагч чиглүүлэлтийг ASA чиглүүлэлтийн хүснэгтэд байгаа эсэхийг баталгаажуулахын тулд **show route** чиглүүлэлтийн командаар гаргана.

```
CCNAS-ASA(config)#show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

C    192.168.1.0 255.255.255.0 is directly connected, inside, Vlan1
C    192.168.2.0 255.255.255.0 is directly connected, dmz, Vlan3
     209.165.200.0/29 is subnetted, 2 subnets
C       209.165.200.0 255.255.255.248 is directly connected, outside,
Vlan2
C       209.165.200.224 255.255.255.248 is directly connected,
outside, Vlan2
S*   0.0.0.0/0 [1/0] via 209.165.200.225
```

Алхам 2: PAT болон сүлжээний объектуудыг ашиглан хаягийн хөрвүүлэлтийг тохируулах.

а. Дотоод сүлжээний объект үүсгэх, дэд сүлжээ, nat командыг ашиглан түүнд шинж чанаруудыг хуваарилна.

```
CCNAS-ASA(config)# object network inside-net / Дотоод сүлжээнд объект үүсгэж байна

CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0 / Дэд сүлжээ үүсгэж байна

CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface / Сүлжээний хаяг хөрвүүлэгч командыг ашиглан гадна, дотор сүлжээнд диманик интерфейсийг олгож байна.

CCNAS-ASA(config-network-object)# end / Дотоод сүлжээнд үүссэн объектоос гарах
```

б. ASA нь орчуулагдах сүлжээ болон **nat** командын бодит параметрүүдийг тодорхойлдог объект хэсэгт тохиргоог хуваана. Эдгээр нь ажиллаж байгаа тохиргооны хоёр өөр газарт гарч ирдэг. NAT объектын тохиргоог **show run** командыг ашиглан харна.

```
CCNAS-ASA(config)#show run
: Saved
:
ASA Version 8.4(2)
!
hostname CCNAS-ASA
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 switchport access vlan 3
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
```

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 209.165.200.226 255.255.255.248
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
!
object network dmz-server
 host 192.168.2.3
object network inside-net
 subnet 192.168.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 209.165.200.225 1
!
access-list OUTSIDE_DMZ extended permit icmp any host 192.168.2.3
access-list OUTSIDE_DMZ extended permit tcp any host 192.168.2.3 eq www
!
!
access-group OUTSIDE_DMZ in interface outside
object network dmz-server
 nat (dmz,outside) static 209.165.200.227
object network inside-net
 nat (inside,outside) dynamic interface
!
aaa authentication telnet console LOCAL

aaa authentication ssh console LOCAL
!
!
username admin password XK9CbN4MkQEI0jdt encrypted
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect icmp
!
service-policy global_policy global
!
telnet 192.168.1.0 255.255.255.0 inside
telnet timeout 10
ssh 192.168.1.0 255.255.255.0 inside
ssh 172.16.3.3 255.255.255.255 outside
ssh timeout 10
!
dhcpd auto_config outside
!
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd dns 209.165.201.2 interface inside
dhcpd enable inside
```

c. PC-B оролдлогоос 209.165.200.225 IP хаягаар R1 fa0/0 интерфейсийг пинг хийх. Пингүүд амжилтгүй болох ёстой. Яагаад гэвэл холбогдох IP хаягийг **ping** хийх үед өгөгдлийг дамжуулж хариу авах “хүсэлтийн хугацаа дууссан” алдаа гарч байна.

д. Орчуулагдсан болон орчуулагдаагүй **hits** харахын тулд ASA дээр **show nat** командаар гаргана.

```
CCNAS-ASA(config)#show nat
Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic inside-net interface
    translate_hits = 4, untranslate_hits = 3
```

Алхам 3: Анхдагч MPF[8] програмын нийтийн үйлчилгээний хяналтын бодлогыг өөрчлөх

Гадна траффикт хяналт хийх стандарт бодлогын газрын зургийг үүсгэж болно. Зөв тохируулсан тохиолдолд зөвхөн дотроос эхлүүлсэн траффикийг гадна интерфейс рүү буцаах боломжтой. Та хяналтын жагсаалтад ICMP нэмэх шаардлагатай.

а. Ангийн газрын зураг, бодлогын газрын зураг, үйлчилгээний бодлогыг бий болгох. Дараах тушаалуудыг ашиглан ICMP траффикийн хяналтыг бодлогын газрын зургийн жагсаалтад нэмэх дараалал.

```
CCNAS-ASA(config)# class-map inspection_default / Ангийн газрын зургийн анхдагч хяналтыг үүсгэж байна
CCNAS-ASA(config-cmap)# match default-inspection-traffic
CCNAS-ASA(config-cmap)# exit / Гарах
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp / icmp шалгах
CCNAS-ASA(config-pmap-c)# exit / Гарах
CCNAS-ASA(config)# service-policy global_policy global
```

б. PC-B-ээс R1 fa0/0 интерфейсийг 209.165.200.225 IP хаягаар **ping** хийх. ICMP-ийн урсгалыг шалгаж, хууль ёсны дагуу буцах хөдөлгөөнийг зөвшөөрч байгаа тул энэ удаад **ping** амжилттай болно.

```
C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.225: bytes=32 time=43ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254
Reply from 209.165.200.225: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 43ms, Average = 15ms
```

[8] Металл замын байгууламж

Гүйцэтгэх ажил 3: DHCP, AAA, SSH-г тохируулах.

Алхам 1: ASA-г DHCP сервер болгон тохируулах

а. DHCP серверт ip хаягийн санг тохируулаад ASA дотор интерфейс дээр идэвхжүүлнэ.

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside / dhcp хаяг олгож байна
```

б. Үйлчлүүлэгчдэд өгөх DNS серверийн IP хаягийг зааж өгнө.

```
CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside / DNS серверийн IP хаягийг зааж байна
```

в. DHCP клиентийн хүсэлтийг идэвхжүүлсэн интерфейс дээр харахын тулд ASA доторх DHCP демоныг идэвхжүүлнэ.

```
CCNAS-ASA(config)# dhcpd enable inside / DHCP демоныг идэвхжүүлж байна
```

д. PC-B-ийг статик IP хаягаас DHCP клиент болгон өөрчилж, IP хаягийн мэдээлэл хүлээн авч байгаа эсэхийг шалгана.

Алхам 2: Орон нутгийн мэдээллийн баазыг нэвтрэлт, танилтад ашиглахын тулд AAA-г тохируулах

а. Хэрэглэгчийн нэрийн командыг оруулаад админ нэртэй дотоод хэрэглэгчийг тодорхойлно. Нууц үгээ тохируулна.

```
CCNAS-ASA(config)# username admin password cisco1234 / Хэрэглэгчийн нэвтрэх нууц үгийг cisco1234 болгов
```

б. SSH хэрэглэгчийн баталгаажуулалтад зориулж орон нутгийн ASA мэдээллийн санг ашиглахын тулд AAA-г тохируулна.

```
CCNAS-ASA(config)# aaa authentication ssh console LOCAL / Мэдээллийн санг ашиглах AAA тохиргоог хийв
```

Алхам 3: ASA руу алсын хандалтыг тохируулах

ASA нь нэг хост эсвэл сүлжээний дотор болон гадна талын хостуудын холболтыг хүлээн авахаар тохируулагдаж болно. Энэ алхам дээр гаднах сүлжээний хостууд зөвхөн SSH-г ашиглан ASA-тай холбогдох боломжтой. SSH sessions дотоод сүлжээнээс ASA руу нэвтрэхэд ашиглаж болно.

а. SSH холболтыг дэмжихэд шаардлагатай RSA түлхүүр хослолыг үүсгэнэ. ASA төхөөрөмжид RSA товчлуурууд бэлэн болсон тул солихыг шаардахад дугаарыг оруулна.

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024 / RSA товчлуурыг солих дугаарыг 1024 болгов
```

АНХААРУУЛГА: Та <Default-RSA-Key> нэртэй RSA товчлуурын хослолыг аль хэдийн тодорхойлсон байна.

Do you really want to replace them? [yes/no]: no / Та тэдгээрийг орлуулахыг үнэхээр хүсч байна уу? [тийм / үгүй]: үгүй

ERROR: Failed to create new RSA keys named / АЛДАА: <Default-RSA-Key> нэртэй шинэ RSA түлхүүрүүдийг үүсгэж чадсангүй

б. ASA-г дотоод сүлжээний аль ч хостоос (192.168.1.0/24) болон гаднах сүлжээн дэх салбар оффис дахь алсын удирдлагын хостоос (172.16.3.3/30) SSH холболтыг зөвшөөрөхөөр тохируулна. SSH завсарлагааны хугацааг 10 минут болгоорой (анхдагч нь 5 минут).

```
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside / Дотоод сүлжээнд IP хаяг олгож байна

CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside / Гадна сүлжээнд IP хаяг олгож байна

CCNAS-ASA(config)# ssh timeout 10 / Завсарлагааны хугацааг 10 минут болгож байна
```

в. PC-C-ээс ASA (209.165.200.226) хүртэл SSH **sessions** байгуулах.

```
PC> ssh -l admin 209.165.200.226
```

д. PC-B-ээс ASA (192.168.1.1) хүртэл SSH sessions байгуулах.

```
PC> ssh -l admin 192.168.1.1
```

Гүйцэтгэх ажил 4: DMZ, Static NAT, ACL-ийг тохируулах

R1 fa0/0 болон ASA гадна интерфейс нь аль хэдийн 209.165.200.225 ба 209.165.200.226-г тус тус ашигладаг.

Алхам 1: ASA дээр DMZ интерфейсийг VLAN 3 тохируулах

а. Олон нийтийн хандалттай вэб сервер байрладаг DMZ VLAN 3-ийг тохируулна. IP хаяг 192.168.2.1/24-ийг оноож, dmz гэж нэрлээд 70-ийн аюулгүй байдлын түвшнийг зааж өгнө. Сервер дотор хэрэглэгчидтэй холбоо эхлүүлэх шаардлагагүй тул VLAN 1 интерфейс рүү дамжуулахыг идэвхгүй болгоно.

```
CCNAS-ASA(config)# interface vlan 3 / Интерфейс сонгож байна

CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0 / IP хаяг олгож байна

CCNAS-ASA(config-if)# no forward interface vlan 1 / vlan 1 интерфейсийг идэвхгүй болгож байна

CCNAS-ASA(config-if)# nameif dmz / Нэр олгож байна
```

INFO: Security level for "dmz" set to 0 by default. / Мэдээлэл: "dmz" -ийн аюулгүй байдлын түвшнийг анхдагчаар 0 гэж тохируулсан болно.

```
CCNAS-ASA(config-if)# security-level 70 / Аюулгүй байдлын тэвшийг 70 гэж тохируулаа
```

б. ASA физик интерфейс fa0 /2-ийг DMZ VLAN 3-д оноож, интерфейсийг идэвхжүүлнэ.

```
CCNAS-ASA(config-if)# interface Ethernet0/2 / Интерфейс сонгож байна
```

```
CCNAS-ASA(config-if)# switchport access vlan 3 / Интерфейсийг идэвхжүүлж байна
```

Алхам 2: Сүлжээний объект ашиглан статик NAT-ийг DMZ сервер дээр тохируулах

Dmz-server нэртэй сүлжээний объектыг тохируулаад DMZ серверийн статик IP хаягийг оноож (192.168.2.3) өгнө. Объектыг тодорхойлох горимд байх үед статик NAT ашиглан DMZ хаягийг гаднын хаягаар хөрвүүлэхэд ашиглагдахыг зааж, нийтийн орчуулсан хаягийг зааж өгнө. (209.165.200.227)

```
CCNAS-ASA(config)# object network dmz-server / DMZ сервер үүсгэж байна

CCNAS-ASA(config-network-object)# host 192.168.2.3 / IP хаяг олгож байна

CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227 / Нийтийн орчуулсан хаягийг оноож байна

CCNAS-ASA(config-network-object)# exit / Гарах
```

Алхам 3: Интернетээс DMZ сервер рүү нэвтрэх боломжийг олгох ACL-ийг тохируулна.

80-р порт дээрх TCP протоколыг гаднын ямар ч хостоос DMZ серверийн дотоод IP хаяг руу нэвтрэхийг зөвшөөрсөн OUTSIDE-DMZ нэртэй хандалтын жагсаалтыг тохируулна. Хандалтын жагсаалтыг ASA гадна интерфейст “IN” чиглэлд оруулна.

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3

CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80 / 80-р порт дээр tcp протоколын IP хаягийг олгож байна

CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

Тэмдэглэл: IOS ACL-ээс ялгаатай нь ASA ACL зөвшөөрлийн мэдэгдэл нь дотоод хувийн DMZ хаяг руу нэвтрэхийг зөвшөөрөх ёстой. Гадаад хостууд нь серверийн нийтийн статик NAT хаягийг ашиглан нэвтэрч, ASA үүнийг дотоод хост IP хаяг руу хөрвүүлж, дараа нь ACL-ийг хэрэглэнэ.

2.5. Боловсруулсан лабораторийн ажил

2.5.1. Сүлжээний галт ханыг тохируулж DMZ сүлжээ үүсгэх

Лабораторийн ажлын зорилго:

Энэхүү лабораторийн ажлаар Галт хана төхөөрөмж дээр үндсэн тохиргоог хийж хооронд нь холбоно.

Лаборатори хийхэд шаардагдах төхөөрөмжүүд:

Cisco packet tracer симуляцын программ

Лабораторийг гүйцэтгэх алхам:

Алхам 1: Сүлжээг холбох

Алхам 2: IP хаягийг тохируулах

Алхам 3: ASA төхөөрөмжийн үндсэн тохиргоо болон интерфейсийн аюулгүй байдлыг тохируулах

Алхам 4: DHCP, AAA, SSH-г тохируулах

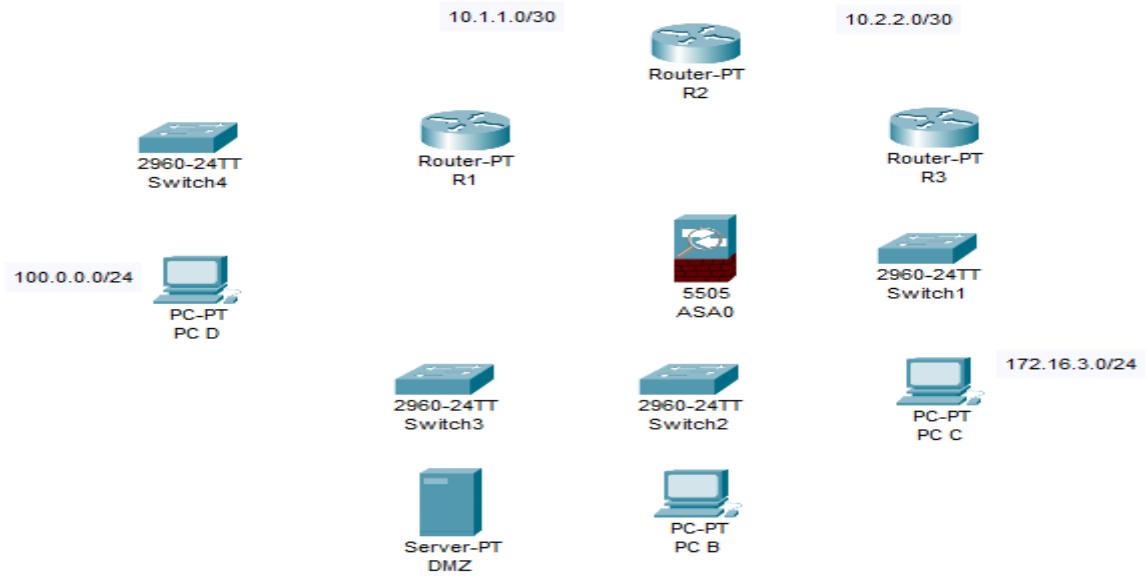
Алхам 5: DMZ, Static NAT, ACL-ийг тохируулах

Алхам 6: Сүлжээний замыг зааж өгөх

Шалгах команд:

- show ip address
- show switch vlan
- show route
- show run
- show nat
- show ip brief
- ping

DMZ сүлжээний логик топологи



Хаягийн хүснэгт

Төхөөрөмж	Интерфейс	IP хаяг	Subnet mask	Гарцын хаяг
Router 0	Se0/0/0	192.168.10.1	255.255.255.252	-
	Gig0/0	192.168.1.1	255.255.255.0	-
Router 1	Se0/0/0	192.168.10.2	255.255.255.252	-
	Se0/0/1	192.168.20.2	255.255.255.252	-
	Gig0/0	192.168.2.1	255.255.255.0	-
Router 2	Se0/0/0	192.168.20.1	255.255.255.252	-
	Gig0/0	192.168.3.1	255.255.255.0	-
PC-0	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-1	NIC	192.168.2.2	255.255.255.0	192.168.2.1
PC-2	NIC	192.168.3.2	255.255.255.0	192.168.3.1

Ажил 1:

Сүлжээг холбо.

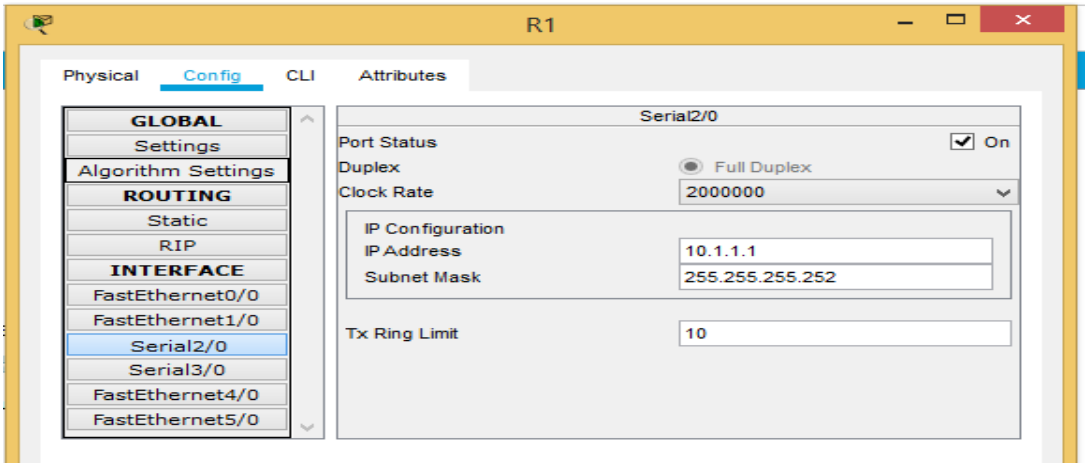
Алхам 1. Зөв кабелийг ашиглан дараах зааврын дагуу сүлжээг холбо.

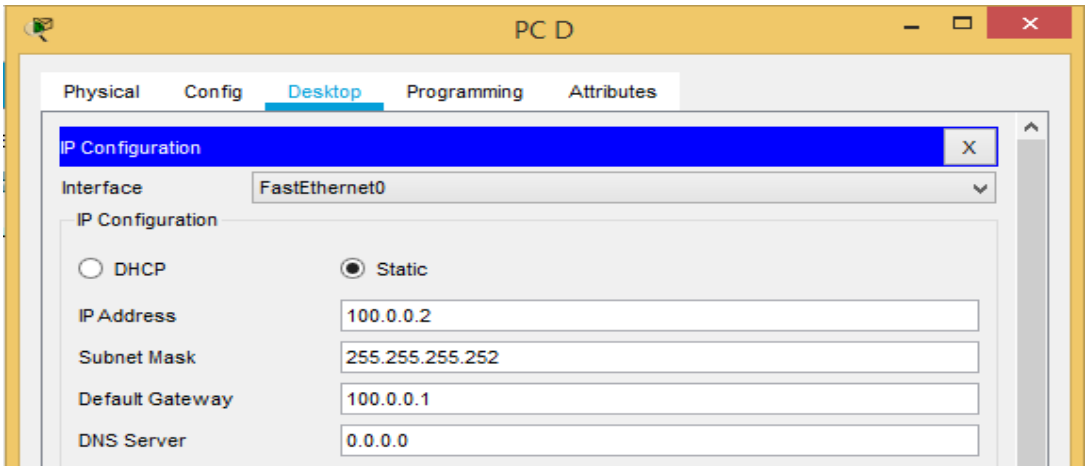
- R1-ийн Se2/0-ийг R2-ийн Serial порттой
- R1-ийн Se3/0-ийг R3-ийн Serial порттой
- R3-ийн Fa0/0-ийг Switch1-ийн FastEthernet порттой
- Switch1-ийн Fa0/2-ийг PC C-ийн FastEthernet порттой
- R1-ийн Fa0/0-ийг ASA-ийн Ethernet порттой
- ASA-ийн Et0/1-ийг Switch2-ийн FastEthernet порттой
- Switch2-ийн Fa0/2-ийг PC B-ийн FastEthernet порттой
- ASA-ийн Et0/2-ийг Switch3-ийн FastEthernet порттой
- Switch3-ийн Fa0/2-ийг DMZ серверийн FastEthernet порттой
- R1-ийн Fa1/0-ийг Switch4-ийн FastEthernet порттой
- Switch4-ийн Fa0/2-ийг PC D-ийн FastEthernet порттой

Ажил 2:

IP хаягийг тохируулах

Алхам 1. Статик сүлжээний хаяг тохируулах (Жишээ)





Ажил 3:

ASA төхөөрөмжийн үндсэн тохиргоо болон интерфейсийн аюулгүй байдлыг тохируулах

Алхам 1. Хостын нэрийг CCNAS-ASA болгон тохируул.

```
ciscoasa>enable/Privileged горимд шилжиж байна.
ciscoasa# config terminal
ciscoasa(config-if)# hostname CCNAS-ASA
```

Алхам 2.Төхөөрөмжид хандах нууц үгийг тохируулах

```
ciscoasa>enable
ciscoasa#config terminal
ciscoasa(config-if)#enable password ciscoenpa55
```

Алхам 3. Дотор болон гадна талын интерфейсийг тохируулах.

- VLAN 1 (дотор) интерфейсийг тохируулах болно.
- VLAN 2 (гадна) интерфейсийг тохируулах болно.

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
CCNAS-ASA(config-if)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# security-level 0
```

Алхам 4. ASA холболтыг шалга.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ажил 4:

DHCP, AAA, SSH-г тохируулах

Алхам 1**.** ASA-г DHCP сервер болгон тохируулах

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside
CCNAS-ASA(config)# dhcpd enable inside
```

Алхам 2**.** Орон нутгийн мэдээллийн баазыг нэвтрэлт, танилтад ашиглахын тулд AAA-г тохируулах

```
CCNAS-ASA(config)# username admin password cisco1234
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
```

Алхам 3. ASA руу алсын хандалтыг тохируулах

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

Ажил 5:

DMZ, Static NAT, ACL-ийг тохируулах

Алхам 1. ASA дээр DMZ интерфейсийг VLAN 3 тохируулах

```
CCNAS-ASA(config)# interface vlan 3
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# no forward interface vlan 1
CCNAS-ASA(config-if)# nameif dmz
CCNAS-ASA(config-if)# security-level 70
CCNAS-ASA(config-if)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
```

Алхам 2. Сүлжээний объект ашиглан статик NAT-ийг DMZ сервер дээр тохируулах

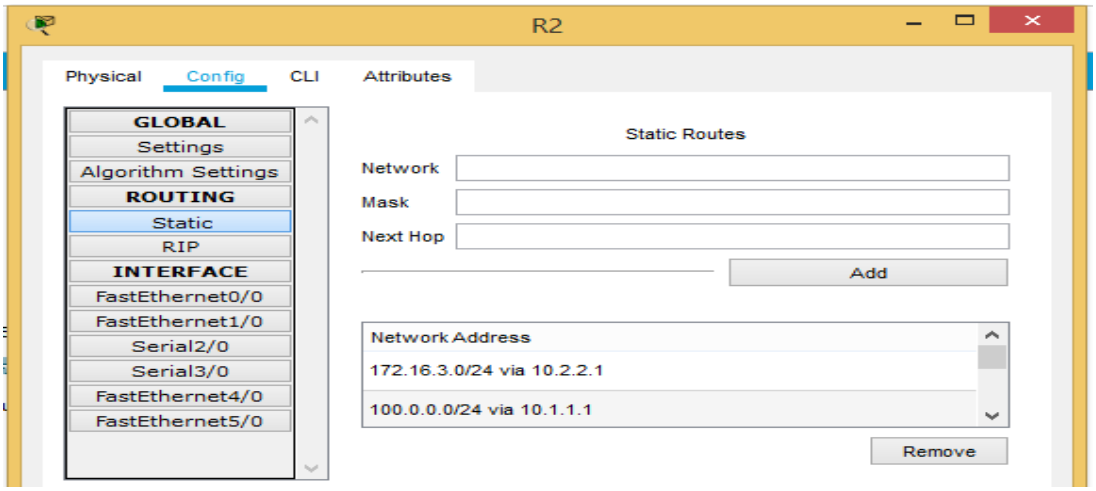
```
CCNAS-ASA(config)# object network dmz-server

CCNAS-ASA(config-network-object)# host 192.168.2.3

CCNAS-ASA(config-network-object)#nat(dmz,outside)static
209.165.200.227

CCNAS-ASA(config-network-object)# exit
```

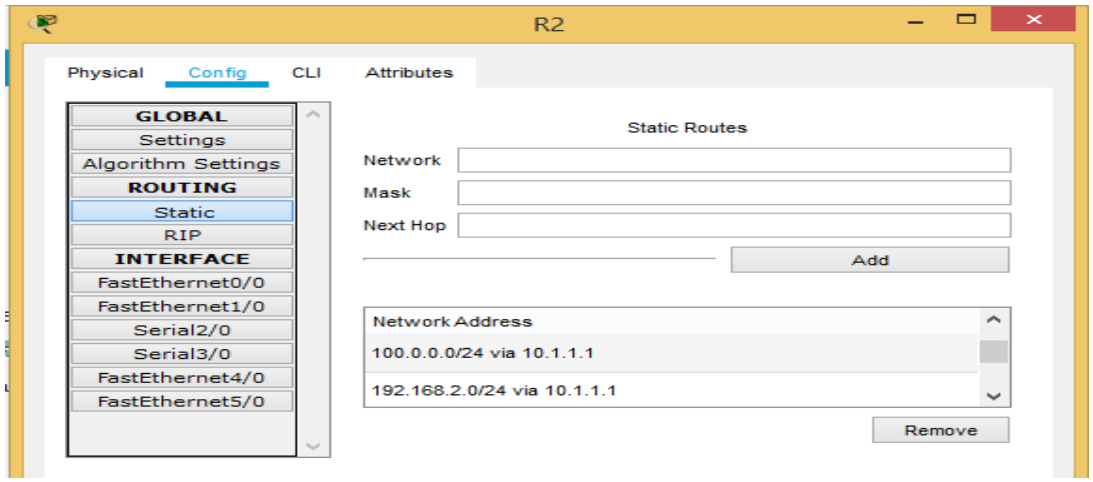
Алхам 3. Интернетээс DMZ сервер рүү нэвтрэх боломжийг олгох ACL-ийг тохируулна.

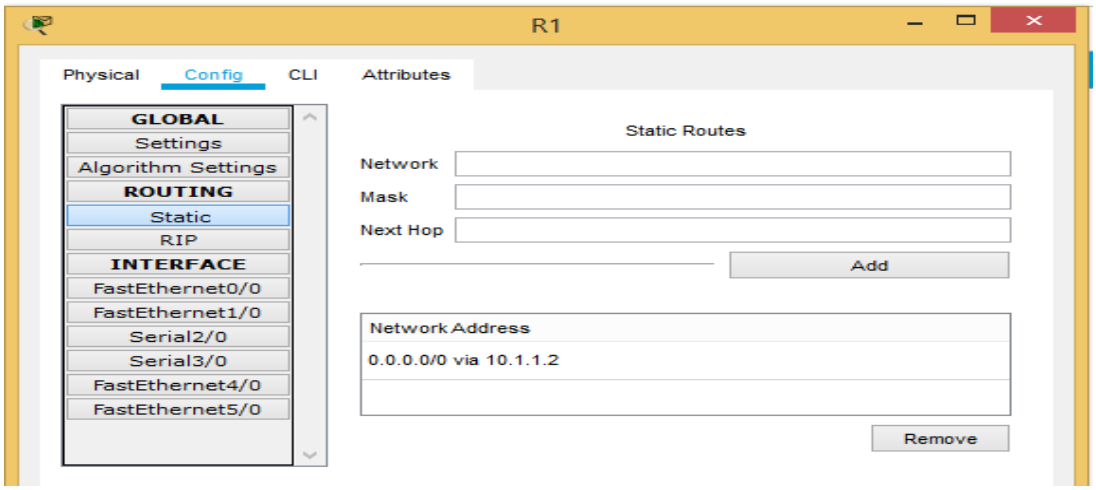
```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host
192.168.2.3

CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host
192.168.2.3 eq 80

CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

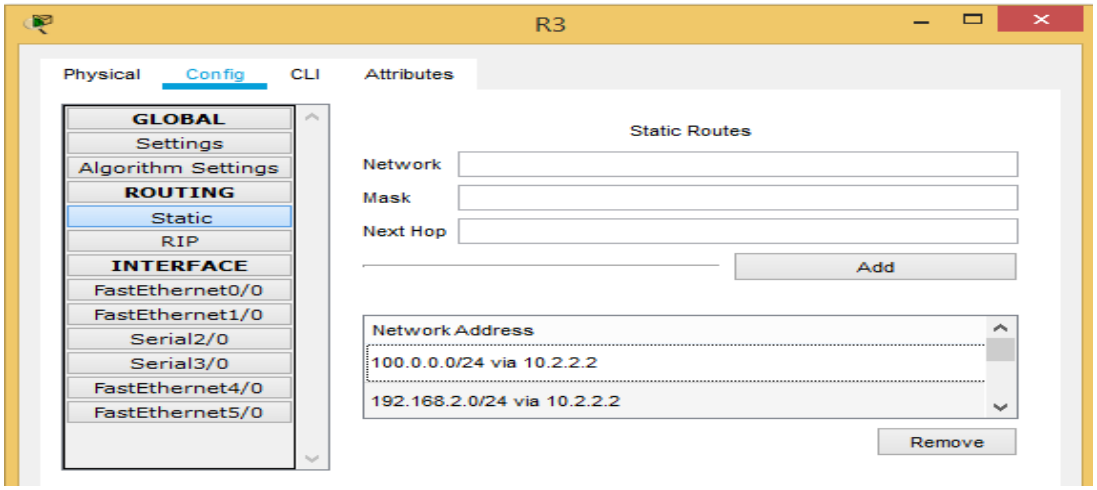
Ажил 5:

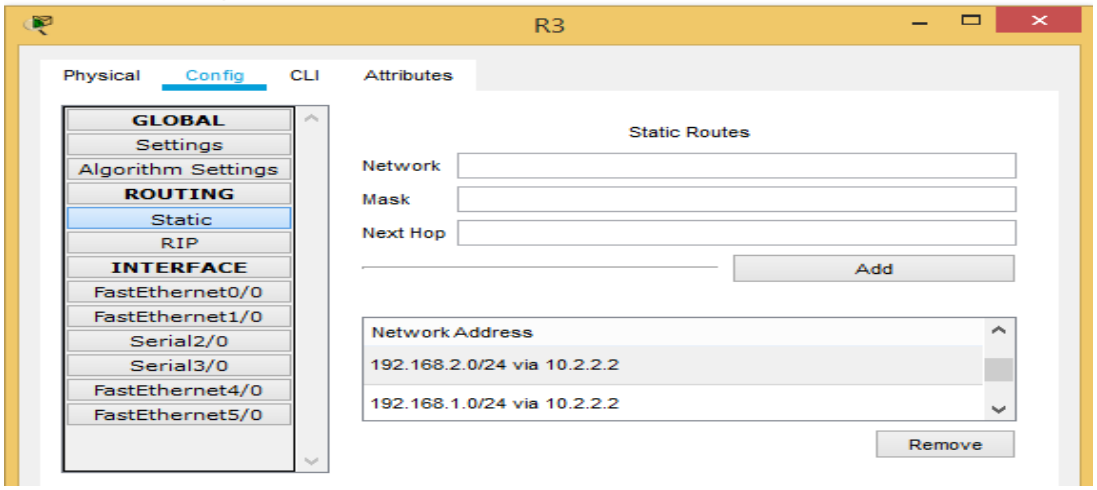
Сүлжээний замыг зааж өгөх






R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
0.0.0.0/0 via 10.1.1.2
Remove


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
100.0.0.0/24 via 10.2.2.2
192.168.2.0/24 via 10.2.2.2
Remove


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Serial2/0
Serial3/0
FastEthernet4/0
FastEthernet5/0
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.2.0/24 via 10.2.2.2
192.168.1.0/24 via 10.2.2.2
Remove

Дүгнэлт

Байгууллага болон аж ахуйн нэгжүүд нь дотоод сүлжээгээ хамгаалахын тулд галт ханыг ашигладаг. Галт хана гаднын халдлагаас дотоод сүлжээг хамгаалах техник хангамж болон программ хангамжийн хослол юм. Галт ханыг дотор нь хэд хэд ангилдаг бөгөөд өөр өөрийн гэсэн гүйцэтгэх үүрэгтэй. Мөн галт хана ашиглан DMZ сүлжээ үүсгэх боломжтой байдаг энэ нь дотоод сүлжээг бусад сүлжээнээс тусгаарлаж сүлжээний үндсэн нөөцийг аюулгүй байлгадаг. Гол санаа нь гаднаас ирэх урсгалыг хянаж дотоод сүлжээг халдлагад өртөхөөс хамгаалах үүрэгтэй.

Энэхүү төгсөлтийн ажлаараа Монгол Улсын Боловсролын Их сургуульд хэрэглэдэг Fortinet компанийн Fortigate 400E галт ханын төхөөрөмжийн талаар дэлгэрэнгүй судаллаа. Fortinet компанийн Fortigate галт хана төхөөрөмж нь хүмүүсийн хэрэгцээ шаардлагад бүрэн нийцсэн дараагийн үеийн галт ханын шийдлийг өөртөө багтааж чадсан бөгөөд бусад галт ханын төхөөрөмжийг бодвол илүү шинэ дэвшилтэд технологийг өөртөө агуулсан байдаг байна. Мөн гаднаас ирэх халдлагыг бүрэн зогсоож чаддагаараа давуу талтай.

DMZ сүлжээ нь нэг галт ханатай, хоёр галт ханатай гэсэн хоёр архитектуртай байдаг. Туршилтын хувьд сургалтын зориулалттай виртуал сүлжээний орчин буюу Cisco packet tracer програмын дэмждэг галт ханыг ашиглан DMZ сүлжээг хоёр архитектурын дагуу үүсгэхээр төлөвлөсөн боловч хоёр галт ханатай DMZ тохируулах тохиргоог энэхүү програм дэмждэггүй болохыг олж мэдсэн. Иймд нэг галт ханатай DMZ сүлжээг тохируулан ажиллуулж үзсэн. Ингэснээр галт хана хэрхэн ажилладаг яаж сүлжээнүүдээ хамгаалдаг, хэрхэн тохиргоо хийдэг талаар мэдэж авсан.

Ингээд энэхүү төгсөлтийн ажлаар тодорхой хэмжээнд туршилт хийж, сүлжээ зохион байгуулсан мөн сүлжээний хамгаалалтын төхөөрөмж хэрхэн ажилладаг, сүлжээг юунаас хамгаалах, яаж хамгаалах зэрэг онолын судалгаа хийснээрээ сүлжээний аюулгүй байдлын талаар цэгцтэй мэдлэгтэй болсон гэж дүгнэж байна.

Ном зүй

Barracuda.com. 2020. What Is A DMZ (Networking)? | Barracuda Networks. [online] Available at: <https://www.barracuda.com/glossary/dmz-network> [Accessed 30 November 2020].

Comparitech. 2020. What Is A NAT Firewall, How Does It Work And When Do You Need One?. [online] Available at: <https://www.comparitech.com/blog/vpn-privacy/nat-firewall/> [Accessed 30 November 2020].

Docplayer.net. 2020. Firewall Architecture - PDF Free Download. [online] Available at: <https://docplayer.net/11223401-Firewall-architecture.html> [Accessed 30 November 2020].

Docplayer.net. 2020. What Is Firewall? A System Designed To Prevent Unauthorized Access To Or From A Private Network. - PDF Free Download. [online] Available at: <https://docplayer.net/13532423-What-is-firewall-a-system-designed-to-prevent-unauthorized- access-to-or-from-a-private-network.html> [Accessed 30 November 2020].

Humanities.mn. 2020. [online] Available at: <https://www.humanities.mn/fileman/Uploads/Iltgel/2017-2018/namar/18-baigaltugs.pdf> [Accessed 30 November 2020].

Itzone.mn. 2020. ITZONE - Дараа Үеийн Аюулгүй Байдлын Нэр Томьёоны Тайлбар. [online] Available at: <https://www.itzone.mn/content/blog/show/53> [Accessed 30 November 2020].

NordVPN. 2020. What Is A NAT Firewall?. [online] Available at: <https://nordvpn.com/blog/what-is-nat-firewall/> [Accessed 30 November 2020].

Itzone.mn. 2020. ITZONE - Fortigate Галт Хана Гэж Юу Вэ?. [online] Available at: <https://www.itzone.mn/content/blog/show/402> [Accessed 22 December 2020].

Itzone.mn. 2020. ITZONE - Fortinet : 2020 Оны Гартнерын Шидэт Квадратын "WAN Edge Infrastructure" Төрөлд Тэргүүлэгчээр Эрэмбэлэгдэв. [online] Available at: <https://www.itzone.mn/content/blog/show/461> [Accessed 22 December 2020].

Itzone.mn. 2020. ITZONE - FORTINET Firewall 4 Дахь Жилдээ Дараалан LEADERS Ангилалд Эрэмбэлэгдлээ. [online] Available at: <https://www.itzone.mn/content/blog/show/466> [Accessed 22 December 2020].

Itzone.mn. 2020. ITZONE - Fortinet Ашиглан Мэдээллийн Аюулгүй Байдлын Байдлын Дэд Бүтцийн Үр Ашгийг Нэмэгдүүлсэн Нь. [online] Available at: <https://www.itzone.mn/content/blog/show/450> [Accessed 22 December 2020].

Itzone.mn. 2020. ITZONE - Fortinet -Ийн Хамгаалалтын Шийдлүүдээс Онцлох Нь. [online] Available at: <https://www.itzone.mn/content/blog/show/202> [Accessed 22 December 2020].

LLC, I., 2020. Fortimail: Secure Email Gateway. [online] Itzone.mn. Available at: <https://itzone.mn/page/fortinet-secure-email-gateway> [Accessed 22 December 2020].

Хавсралт

Хүснэгт 1. 3 Сүлжээнд ашиглагддаг нэр томъёоны тайлбар

Товчилсон үг		Тайлбар
DCE	Data Communications Equipment	Мэдээлэл холбооны тоног төхөөрөмж (DCE) нь өгөгдлийн эх үүсвэр ба хүрэх газрын хоорондох харилцаа холбооны сүлжээг бий болгох, засварлах, зогсооход ашигладаг.
NIC	Network Interface Controller	Сүлжээний интерфэйсийн хянагч (NIC) нь компьютерийг сүлжээнд холбодог.
ISP	Internet Service Provider	Интернэт үйлчигээ үзүүлэгч нь интернэтэд нэвтрэх , ашиглах эсвэл түүнд оролцох үйлчилгээ үзүүлдэг байгууллагыг хэлнэ.
CLI	Command-line Interface	Тушаалын мөрийн интерфэйс нь командын програмбг текстийн мөр хэлбэрээр боловсруулдаг.
MPF	Metallic Path facility	Металл замын байгууламж (MPF) нь орон нутгийн телефон хэрэглэгчдэд хүргэх үндсэн түгээлтийг дамжуулдаг хамгаалалтгүй эрчилсэн хос утас юм.
PAT	Port Address Translation	Порт хаягийн хөрвүүлэгч. Хувийн IP хаягийг нийтийн IP хаяг руу портын дугаараар хөрвүүлдэг.
ACL	Access Control List	Компьютерийн файлын системийн хандалтыг хянах жагсаалт юм. ACL нь хэрэглэгчид системийн процесс, объектуудад нэвтрэх эрх олгогдсон эсэх, ямар үйлдэл хийж болохыг зааж өгдөг.
NAT	Network Address Translation	Сүлжээний хаяг хөрвүүлэгч (NAT). Хувийн IP хаяг эсвэл орон нутгийн хаягийг нийтийн IP хаяг болгон хөрвүүлдэг.
ICMP	Internet Control Message Protocol	Интернэтийн прокотолын багцад туслах протокол юм. Энэ нь сүлжээний төхөөрөмжүүдийн доторх чиглүүлэгчид IP хаягтай холбогдоход алдаа гарсан тухай үйлдлийн мэдээлэл илгээхэд ашигладаг.
TCP	Transmission Control Protocol	Интернэт протокол програмуудын гол протоколуудын нэг юм.
UDP	User Datagram Protocol	Компьютерийн сүлжээний тээвэрлэлтийн түвшний найдваргүй,

		холболтгүй нөхцөлд хэрэглэгддэг протокол юм.
SSH	Secure Shell	Сүлжээний үйлчилгээг найдвартай хамгаалалтгүйгээр ажиллуулах криптограф сүлжээний протокол юм.
DHCP	Dynamic Host Configuration Protocol	Интернет протокол сүлжээнд хэрэглэгддэг сүлжээний менежментийн протокол юм. DHCP сервер нь сүлжээний төхөөрөмж бүрд IP хаягийг динамикаар хуваарилдаг.
DNS	Domain Name System	Интернет, хувийн сүлжээнд холбогдсон компьютер болон үйлчилгээний нөөц төвлөрсөн системийг нэрлэнэ. Энэ нь аж ахуй нэгж бүр өөрийн гэсэн домэйн нэртэй байна.
PDA	Personal Digital Assistant	Хувийн дижитал туслах буюу гар компьютер гэж нэрлэдэг. Хувийн мэдээллийн менежерийн үүргийг гүйцэтгэдэг төрөл бүрийн хөдөлгөөнт төхөөрөмж юм.
DLP	Data Loss Prevention	Мэдээллийг алдахаас урьдчилан сэргийлэх бөгөөд өгөгдлийн зөрчлийг илрүүлж, хяналт тавих үүрэгтэй.
BYOD	Bring Your Own Device	Хувийн эзэмшлийн төхөөрөмжөө ашиглахыг зөвшөөрдөг.
SIEM	Security Information Event Management	Програм хангамжийн бүтээгдэхүүн, үйлчилгээ нь аюулгүй байдлын мэдээллийн менежмент (SIM) болон аюулгүй байдлын үйл явцын менежмент (SEM) – ийг хослуулан компьютерийн аюулгүй байдлын салбар дахь дэд хэсэг болдог юм.
SSL	Secure Sockets Layer	SSL нь шифрлэлтэд суурилсан интернет аюулгүй байдлын протокол юм. Өндөр нууцлалыг хангахын тулд SSL нь вэбээр дамждаг өгөгдлийг шифрлэдэг.
VPN	Virtual Private Network	Виртуал хувийн сүлжээ нь нийтийн сүлжээгээр дамжин хэрэглэгчдэд өгөгдөл илгээх, хүлээн авах боломжийг олгодог.