សាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ
និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច

សារណាបញ្ចប់ការសិក្សា

ការការពារនិទ្ទេសយអ្នកប្រើប្រាស់ក្នុងប្រព័ន្ធណែតភ្ជឹក

ស្រាវជ្រាវពីថ្ងៃទី១៦ ខែមីនា ឆ្នាំ២០២០ ដល់ថ្ងៃទី១៥ ខែឧសភា ឆ្នាំ២០២០

តាក់តែងឡើងដោយ	សាស្ត្រាចារ្យណែនាំ
និស្សិតឈ្មោះ គង់ រក្សា	បណ្ឌិត លឹម សេងឌី
សន សំខាន់	

ថ្នាក់បរិញ្ញាបត្រ	សេដ្ឋកិច្ចព័ត៌មានវិទ្យា	ឆ្នាំចូលសិក្សា	២០១៦
ជំនាន់ទី	១៥	ឆ្នាំសរសេរសារណា	២០២០

សេចក្តីថ្លែងអំណរគុណ

យើងខ្ញុំឈ្មោះ **គង់ រក្សា** និង **សន សំខាន់** ជានិស្សិតនៃមហាវិទ្យាល័យ សេដ្ឋកិច្ចព័ត៌មានវិទ្យា ថ្នាក់បរិញ្ញាបត្រសេដ្ឋកិច្ចព័ត៌មានវិទ្យា ឆ្នាំទី៤ ជំនាន់ទី១៥ នៃសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច។

សូមសម្តែងនូវកតញ្ញូតាធម៌ និងថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅ ជូនចំពោះ

លោកឪពុក អ្នកម្តាយ ដែលបានផ្តល់កំណើតចិញ្ចឹមបីបាច់ថែរក្សា តាំងពីតូចរហូតមកដល់ថ្ងៃនេះ អប់រំប្រៀនប្រដៅឲ្យស្គាល់ អ្វីខុស អ្វីត្រូវ ល្អ អាក្រក់ ស ឬខ្មៅ ជុំរុញលើកទឹកចិត្តក្នុងការសិក្សា ហើយថែមទាំងជួយទំនុកបម្រុងសព្វគ្រប់បែបយ៉ាង ទាំងស្មារតី សម្ភារៈ និងថវិកា ដើម្បីផ្តល់អោយយើងខ្ញុំមានលទ្ធភាពគ្រប់គ្រាន់ក្នុងការបន្តការសិក្សា ក្រេបយកចំណេះដឹង តាំងពីថ្នាក់មត្តេយ្យសិក្សា រហូតដល់ឧត្តមសិក្សា។ លោកទាំងពីរបានខិតខំតស៊ូ នឿយហត់គ្រប់បែបយ៉ាងដើម្បីអោយកូនៗមានចំណេះដឹងគ្រប់គ្រាន់ក្នុងការជួយទំនុកបម្រុងក្នុង គ្រួសារ និងសង្គមជាតិនៅពេលអនាគត។

ឯកឧត្តម សាកលវិទ្យាធិកា សាកលវិទ្យាធិការង ព្រឹទ្ធបុរស ព្រឹទ្ធបុរសរង ប្រធានការិយាល័យស្រាវជ្រាវ សាស្ត្រាចារ្យ ព្រមទាំងបុគ្គលិកទាំងអស់ នៅក្នុងសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ដែលបានចំណាយពេលវេលាដ៏មានតម្លៃដើម្បីខិតខំបង្ហាត់បង្រៀន ក៏ដូចជាណែនាំយើងខ្ញុំកន្លងមកយ៉ាងយកចិត្តទុកដាក់ និងអស់ពីកម្លាំងកាយចិត្ត។

លោកសាស្ត្រាចារ្យ **ឈឹម សេងឌី** ដែលជាសាស្ត្រាចារ្យណែនាំបានខិតខាំប្រឹងប្រែងអស់ពីកម្លាំងកាយចិត្ត ក្នុងការបង្ហាត់បង្រៀន ផ្តល់ជាចំណេះដឹង ឯកសារ គំនិត គន្លឹះល្អ ព្រមទាំងជួយកែលម្អរាល់នូវកហុសឆ្គងទាំងឡាយរបស់យើងខ្ញុំ ដើម្បីចងក្រងជាសៀវភៅនេះឡើងតាំងពីដើមរហូតដល់ចប់បានដោយជោគជ័យ។

មិត្តភក្តិទាំងអស់ ដែលបានសិក្សាជាមួយគ្នាកន្លងមក។ ពួកគេតែងតែផ្តល់ជាយោបល់ផ្សេងក្នុងការសិក្សា និងជួយទុកធុរៈគ្នាទៅវិញទៅមកនៅពេលមានបញ្ហាផ្សេងៗ ហើយពួកគេក៏តែងតែលើកទឹកចិត្តយើងខ្ញុំក្នុងការរៀបចំសៀវភៅនេះឡើងផងដែរ។

ជាចុងបញ្ចប់យើងខ្ញុំទាំងពីរ សូមប្រសិទ្ធិពរជ័យជូនដល់ លោកអ្នកមានគុណទាំងពីរ ឯកឧត្តម សាកលវិទ្យាធិកា សាកលវិទ្យាធិការង ព្រឹទ្ធបុរស ព្រឹទ្ធបុរសរង ប្រធានការិយាល័យស្រាវជ្រាវ

សាស្ត្រាចារ្យ ព្រមទាំងបុគ្គលិកទាំងអស់នៅក្នុងសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច លោកសាស្ត្រាចារ្យ លឹម សេងឌី និងមិត្តភក្តិទាំងអស់ សូមអោយមានសុខភាពល្អ ទៅណាមកណាប្រកបដោយសុវត្ថិភាពគ្រប់ទីកន្លែង មានសុភមង្គលក្នុងក្រុមគ្រួសារ និងជួបប្រទះតែពុទ្ធពរទាំងបួនប្រការគឺ អាយុ វណ្ណៈ សុខៈ ពលៈ កុំបីឃ្លៀងឃ្លាតឡើយ។

អារម្ភកថា

ក្រោយពីបានបញ្ចាប់ការសិក្សាផ្នែកទ្រឹស្តីនៃជំនាញសេដ្ឋកិច្ចព័ត៌មានវិទ្យានៅសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រនិងវិទ្យាសាស្ត្រសេដ្ឋកិច្ចរយៈពេលជាងបីឆ្នាំកន្លងមកនេះយើងខ្ញុំបានចំណាយពេលវេលាក្នុងការសិក្សា ស្រាវជ្រាវនិងចងក្រងជាសៀវភៅនេះឡើងដែលជាការធ្វើការស្រាវជ្រាវលើប្រធានបទ៖ **ការការពារទិន្នន័យអ្នកប្រើប្រាស់ក្នុងប្រព័ន្ធណែតវឺក** ដើម្បីបញ្ជាក់ថាបានបញ្ចប់ថ្នាក់បរិញ្ញាបត្រផ្នែកសេដ្ឋកិច្ចព័ត៌មានវិទ្យានៅសាកលវិទ្យាល័យភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច។

ស្នាដៃនេះបានបង្កើតចេញពីការខិតខំប្រឹងប្រែងស្រាវជ្រាវរបស់យើងខ្ញុំទាំងពីររូប រួមសហការជាមួយសាស្ត្រាចារ្យណែនាំ ព្រមទាំងមិត្តភក្តិដែលជួយផ្តល់ជាមិតិផ្សេងៗ។ យើងខ្ញុំចងក្រងសៀវភៅនេះឡើង ដើម្បីជួយកាត់បន្ថយនូវហានិភ័យផ្សេងៗដែលមានការកើតឡើងនៅក្នុងបណ្តាញណែតវឺក និងព្រមទាំងការការពារទិន្នន័យរបស់អ្នកផងដែរ។ ហើយយើងទាំងពីរនាក់ក៏មានបំណង លើកស្ទួយការធ្វើការស្រាវជ្រាវលើវិស័យព័ត៌មានវិទ្យាអោយកាន់តែច្រើនបន្តទៀតនៅក្នុងប្រទេសកម្ពុជា ដើម្បីទុកជាសមិតិផលដល់អ្នកស្រាវជ្រាវជំនាន់ក្រោយផងដែរ។

សៀវភៅនេះក៏ជាគុណប្រយោជន៍របស់អ្នកស្រាវជ្រាវជំនាន់ក្រោយរបស់និស្សិត និងអ្នកផ្សេងទៀត ដែលចង់សិក្សាស្វែងយល់ពីបច្ចេកវិទ្យាដែលមាននៅក្នុងផ្នែកព័ត៌មានវិទ្យា ហើយវាក៏ជាសមិតិផលដំបូងរបស់ពួកខ្ញុំផងដែរ ទោះបីយើងខ្ញុំខិតខំធ្វើការសម្រិតសម្រាំង និងពិនិត្យម៉ត់ចត់យ៉ាងណាក៏ដោយ ក៏យើងខ្ញុំនៅតែជឿជាក់ថាសៀវភៅមួយនេះនៅតែមានកំហុសឆ្គង ឬ ខ្វះចន្លោះដោយយថាហេតុ ឬដោយអចេតនាជាមិនខាន។

ជាទីបញ្ចប់ យើងខ្ញុំទាំងពីរនាក់សូមប្រសិទ្ធិពរជូនពរដល់អ្នកអានទាំងអស់ ទទួលបាននូវពុទ្ធពរទាំងបួនប្រការនៅក្នុងជីវិតអ្នកទាំងអស់គ្នាតរៀងទៅ ទៅណាមកណាប្រកបដោយសុវត្ថិភាព និងមានសុភមង្គលនៅក្នុងគ្រួសារ។ ម្យ៉ាងវិញទៀតយើងខ្ញុំសូមទទួលការរិះគន់ និងកែលំអទាំងឡាយដោយក្តីសោមនស្ស ពីសំណាក់អ្នកអានទាំងអស់គ្នា។

មាតិកា

សេចក្តីសន្និដ្ឋាន និង ការផ្តល់អនុសាសន៍

ឯកសារយោង

បញ្ជីរូបភាព

សេចក្តីផ្តើម

១. សំនាំដើម

នាពេលបច្ចុប្បន្ននេះ យើងដឹងហើយថាពិភពលោកមានការអភិវឌ្ឍន៍យ៉ាង ឆាប់រហ័សនៅគ្រប់វិស័យជាពិសេសដូចជាវិស័យបច្ចេកវិទ្យាព័ត៌មានវិទ្យា ដែលបានដើរតួនាទីយ៉ាងសំខាន់មួយក្នុងការធ្វើឲ្យមានទំនាក់ទំនងរវាងគ្នានឹងគ្នា។ តាមរយៈការរីកចម្រើននេះធ្វើឲ្យ វាមានភាពកាន់តែងាយស្រួលក្នុងការទំនាក់ទំនងយ៉ាងរហ័សមួយផងដែរ។ ដោយសារតែការប្រើប្រាស់បច្ចេកវិទ្យាព័ត៌មានវិទ្យា មានភាពទំលំទូលាយ បែបនេះហើយ ទើបមានការប្រើប្រាស់ មុខងារ ជាច្រើនតាមរយៈការប្រើប្រាស់បណ្តាណាណែតរ៉ឹក សម្រាប់ការដែលមានប្រយោជន៍សម្រាប់ស្តាបន័ជាច្រើន ។ តាមការប្រើប្រាស់ ប្រព្ធន័បណ្តាញណែតរ៉ឹកដែលមានលក្ខណៈដូចជា បណ្តាញណែតរ៉ឹក លក្ខណតូច បណ្តាញណែតរ៉ឹកលក្ខណៈមធ្យម នឹង បណ្តាញណែតរ៉ឹកលក្ខណៈទំលំទូលាយ ។ ការប្រើប្រាស់បណ្តាញណែតរ៉ឹក វាមានភាពប្រហាក់ប្រហែលគ្នាច្រើន ដូចជាអាចគ្រប់គ្រង់ទិន្នន័យពីការវាយប្រហារពីជនខិលខូចខាងក្រៅ ងាយស្រួលក្នុងការផ្ទេរទិន្នន័យច្រើននឹងការងារដែលមានប្រយោជន៍ជាច្រើនទៀត។ ដោយសារកត្តាទាំងនេះដែលអាចធ្វើឲ្យស្តាបន័រដ្ឋ នឹងឯកជនជាច្រើន ប្រើប្រាស់ប្រព្ធន័មួយនេះស្ទើរតែគ្រប់ផ្នែកទាំងអស់ក្នុងស្តាបន័របស់ពួកគេ ។ ហេតុដូចនេះហើយ ទើបធ្វើឲ្យក្រុមរបស់ខ្ញុំមានគំនិត ក្នុងការសិក្សាស្រាវជ្រាវអំពីប្រព្ធន័ណែតរ៉ឹក ដែលជាបច្ចេកវិទ្យាមួយដែល មានភាពងាយស្រួសក្នុងការធ្វើឲ្យមានទំនាក់ទំនង នឹងសិក្សាស្រាវជ្រាវអំពីសុវត្ថិភាពក្នុងការដឹងពីប្រើប្រាស់ប្រព្ធន័ណែតរ៉ឹកមួយនេះ ឲ្យប្រសិទ្ធភាព តាមរយៈវិធានបទ " ការការពារប្រព្ធន័សុវិត្ថភាពណែតរ៉ឹក " ដែលជំរុញឲ្យមានការការពារទុកជាមុនក្នុងការប្រើប្រាស់ណែតរ៉ឹកឲ្យមានសុវត្ថិភាព នឹងប្រសិទ្ធភាពមួយ។

២. មូលដ្ឋាននៃការសិក្សាស្រាវជ្រាវ

តាមរយៈការប្រើប្រាស់បណ្តាញណែតរ៉ឹក តែងតែមានការរំខានពីជនខិលខូចដែលព្យាយាមលួចយកឯកសាររបស់យើង ដូចនេះការការពារប្រព្ធន័សុវត្ថិភាពណែករ៉ឹក គឺជាកត្តាមួយដែលអាចធានាបាននូវសុវត្ថិភាពទិន្នន័យរបស់អ្នកកំឡុងពេលដែលអ្នកប្រើប្រាស់បណ្តាញណែតរ៉ឹកឲ្យមានភាពល្អប្រសើរ។ លើសពីនេះទៅទៀតអ្នកគ្រប់គ្រង់លើប្រព្ធន័នេះអាចប្រើប្រាស់ប្រព្ធន័បណ្តាញណែតរ៉ឹកនេះសម្រាប់ការគ្រប់គ្រង់ ឬអាចបញ្ជ ព្រមទាំងអាចអនុញ្ញាតឲ្យត្រឹមតែអ្នកប្រើប្រាស់បាន

ប្រើប្រាស់នូវទំហំការងាររបស់ពួកគេតែប៉ុណ្ណោះ ដោយមិនអនុញ្ញាតឲ្យអ្នកប្រើប្រាស់អាចធ្វើអ្វីដែលមានផលប៉ះពាល់ដល់ប្រព្ធន័ណែតវ៉ឹកនោះឡើយ។

៣. ការកំណត់បញ្ហានៃការស្រាវជ្រាវ

ផ្អែកទៅការសិក្សាស្រាវជ្រាវលើការប្រើប្រាស់បណ្តាញណែតវ៉ឹក វាតែងតែកើតឡើងនូវបញ្ហាមួយចំនួនដែលភាគច្រើនបង្ករឡើងដោយពួក HACKER ដែលតែងតែរំខាន វាយប្រហារ នឹងលួចទិន្នន័យនៅតាមបណ្តាញណែតវ៉ឹកដែលបានប្រើប្រាស់។ ជនទាំងនេះតែងតែប្រើប្រាស់នូវកម្មវិធីដែលមានផ្ទុកមេរោគ ដើម្បីផ្សាយមេរោគទាំងអស់នេះក្នុងកុំព្យូទ័រ រួចក៏គ្រប់គ្រងរាល់សកម្មភាពដែលយើងបានប្រតិបត្តិ។ ហើយមេរោគទាំងនេះវាអាចជ្រៀតចូលបាននៅពេលដែលយើងមិនមានការប្រុងប្រយ័ត្ននៅពេលដែលយើងបានប្រើប្រាស់ អ៊ិនធឺណែត ឬមានការធ្វេសប្រហែសក្នុងប្រការណាមួយ ដូចជាការ ទាញកម្មវិធី ដែលមានមេរោគពីប្រព្ធន័អ៊ិនធឺណែត។ ព្រមទាំងការប្រើប្រាស់ប្រព្ធន័ អ៊ិនធឺណែតដោយគ្មានឧបករណ៍ ទប់ស្កាត់ពីការវាយប្រហាររបស់ ATTACKER ដូចជាឧបករណ៍ការពារ CISCO FIREWALL ជាដើម។

៤.គោលបំណងនៃការស្រាវជ្រាវ

តាមរយៈនៃការស្រាវជ្រាវលើផ្អែកណែតវ៉ឹក ក្រុមយើងខ្ញុំមើលឃើញនូវការប្រើប្រាស់នូវ Tools មួយចំនួនសម្រាប់តំឡើង ដើម្បីការពារនូវសុវត្ថិភាពទិន្នន័យ ក៏ដូចជាកាត់បន្ថយនូវការវាយប្រហារនានាពី ATTACKER ព្រមទាំងអាចគ្រប់គ្រងនូវអ្នកប្រើប្រាស់មានស្ថិទ្ធត្រឹមតែអាចធ្វើកិច្ចការរបស់ពួកគេតែប៉ុណ្ណោះ។ ខាងក្រោមនេះជាចំណុចសំខាន់ៗដែលយើងបានសិក្សាស្រាវជ្រាវ៖

- គ្រប់គ្រងទៅលើគណនីអ្នកប្រើប្រាស់ និង កំណត់សិទ្ធិប្រើប្រាស់
- ការពារលើ បណ្តាញណែតវ៉ឹកធុរកិច្ចតូចៗ
- ការការពារទៅលើទិន្នន័យរបស់អ្នកប្រើប្រាស់
- ធ្វើការតំឡើង បណ្តាញណែតវ៉ឹកនៅក្នុងផ្ទះ

៥. វិធីសាស្ត្រនៃការស្រាវជ្រាវ

ក្រោយពីការវិភាគ ក៏ដូចជាការសិក្សាស្រាវជ្រាវទៅលើប្រធានបទខាងលើនេះ យើងមានវិធីសាស្ត្រដែល គ្រាំទ្រលើ ការសិក្សា បែប រុករកឯកសារ ដែលមានក្នុង បណ្ណាល័យ ក្នុងបណ្តាញអ៊ីនធើណែត ក៏ដូចជាឯកសារដែលបានសិក្សាម្តងរួចមកហើយ ដែលជាប្រភពសំខាន់ក្នុងការ

គ្រាំទ្រលើប្រធានបទរបស់យើងខាងលើនេះ។យើងបានចែកជាដំណាក់កាលក្នុងការធ្វើវិធីសាស្ត្រក្នុងការស្រាវជ្រាវដែលអាចនាំឲ្យយើងមានភាពងាយស្រួលសម្រាប់ប្រធានបទរបស់យើង។
ដំណាក់កាលទាំងនោះរួមមាន៖

- ស្វែងយល់ពីចំណុចខ្សោយនៃណែតវឹក ដែលយើងត្រូវការពារ
- រៀបរៀងរាល់សំណួរដែលពាក់ព្ន័លើការការពារប្រព្ន័ណែតវឹក
- ការស្វែងរកឯកសារដែលមានក្នុងបណ្ណាល័យ នឹង ប្រព្ន័ណែតវឹក
- ការអនុវត្តលើការវាយប្រហារ នឹងការការពារលើកម្មវិធីផ្សេងៗ

៦. ដែនកំណត់នឹងវិសាលភាពនៃការសិក្សាស្រាវជ្រាវ

ផ្អែកទៅតាមពេលវេលានៃការសិក្សាស្រាវជ្រាវលើប្រធានបទខាងលើ ដែនកំណត់នៃការយល់ដឹងនៃការការពារប្រព្ន័ណែតវឹកយើងអាចត្រឹមតែបាននូវចំណុចស្នូលខ្លះៗ នៃប្រធានបទខាងលើនេះផងដែល ដូចជា ការការពារលើប្រព្ន័កុំព្យូទ័រ ការដាក់ប្រព្ន័លេខសម្ងាត់ដែលខ្លាំង ការបើកដំណើរការនៃ FIREWALL នឹង WINDOW DEFENDER ជាដើម ។ ការសិក្សាលើការដាក់ COMMAND នៅលើឧបករណ៍ដែលបានប្រើប្រាស់ក្នុងប្រព្ន័ណែតវឹក។ ចំពោះវិសាលភាពនៃការសិក្សាស្រាវជ្រាវរបស់ក្រុមយើងខ្ញុំ គ្រាន់តែផ្តោតសំខាន់លើ ហាងកាហ្វេតូចតាច នឹង លើក្រុមហ៊ុនកំរិតតូចតែប៉ុណ្ណោះ ។

៧. សារៈសំខាន់ក្នុងស្រាវជ្រាវ

ផ្អែកលើការសិក្សាស្រាវជ្រាវលើប្រធានបទខាងលើយើងបានរួមនូវសារៈសំខាន់មួយចំនួនដែលល្អក្នុងការការពារ ប្រព្ន័សុវត្ថិភាពណែតវឹកដូចជា៖

- ការពារទិន្នន័យដែលបានផ្ទេរតាមរយៈអ៊ីនធើណែត កុំឲ្យមានការបាត់បង់
- ការពារផ្ទាល់ទិន្នន័យក្នុងកុំព្យូទ័រ
- បង្កើននូវការប្រុងប្រយ័ត្នក្នុងការប្រើប្រាស់ប្រព្ន័ណែតវឹក

៨. រចនាសម្ព័ន្ធនៃការសិក្សាស្រាវជ្រាវ

ដើម្បីសិក្សាពីប្រធានបទខាងលើនេះ យើងរៀបរចនាសម្ព័ន្ធជាចំណុចធំៗបី គឺ ការសិក្សាលើសេចក្តីផ្តើមការសិក្សាលើទ្រឹស្តីនៃណែតវឹក ការសិក្សាពីការការពារលើប្រព្ន័ណែតវឹក ។

- ការសិក្សាលើសេចក្តីផ្តើម

- កំណត់បញ្ហានៃប្រព្ធន័ណែតវឹក
- ស្វែងរកគោលបំណងនៃការការពារ
- ដឹងពីសារៈប្រយោជន៍នៃការការពារណែតវឹក

➢ ការសិក្សាលើទ្រឹស្តីនៃណែតវឹក

- ស្គាល់ពីប្រភេទនៃណែតវឹក
- ស្គាល់ពីប្រភេទឧបករណ៍នៃការប្រើ

➢ ការសិក្សាលើការពារលើប្រព្ធន័ណែតវឹក

- ការពារកុំព្យូពីជ្រៀតចូលនៃប្រភេទនៃមេរោគ
- ការពារទិន្នន័យរបស់កុំព្យូទ័រលើអ៊ីនធើណែត

ជំពូកទី១
ការសិក្សាទ្រឹស្តីបណ្តាញឈែតខ្ទឹក

១.១ មូលដ្ឋានគិតគោលការណ៍សន្តិសុខ (Security Concepts and Principles)

គោលបំណងនិងវត្ថុបំណងសំខាន់នៃ សន្តិសុខប្រព័ន្ធព័ត៌មាន គឺស្ថិតនៅលើគោលការណ៍សន្តិសុខបីគឺ ភាពសម្ងាត់ សុក្រឹតភាព និង លទ្ធភាព (CIA Triad)។

១.១.១ ភាពសម្ងាត់ (Confidentiality)

គោលការណ៍សំខាន់ទី១នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺភាពសង្ងាត់។ ភាពសម្ងាត់គឺជាការថែរក្សាការសម្ងាត់ឬឯកជនភាពរបស់បុគ្គលឬស្ថាប័ន ដើម្បីធានាថាព័ត៌មានសំខាន់ៗអាចអាក់សេសបាន លុះត្រាតែមានសិទ្ធិ។ វាជាគំនិតមួយនៃវិធានការណ៍សន្តិសុខដែលត្រូវបានប្រើដើម្បីធានាការការពារការសម្ងាត់ទិន្នន័យ វត្ថុ ឬ ធនធាននៅលបណ្តាញកុំព្យូទ័រឬប្រព័ន្ធ។ គោលដៅនៃការ ការពារភាព សម្ងាត់គឺ ដើម្បី ការពារឬកាត់បន្ថយ អាក់សេស ទិន្នន័យដោយ គ្មានការអនុញ្ញាត។

១.១.២ សុក្រឹតភាព (Integrity)

គោលការណ៍សំខាន់ទី២នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺសុក្រឹតភាព។ វាជាភាពត្រឹមត្រូវនៃព័ត៌មានដែលទទួលបានធៀបនឹងព័ត៌មានដើមដែលផ្ទុកក្នុងកុំព្យូទ័រ ជាពិសេស ពេលធ្វើចរាចរណ៍លើបណ្តាញកុំព្យូទ័រ។ សុក្រឹតភាពគឺជាគំនិតនៃការការពារភាពជឿជាក់និងភាពត្រឹមត្រូវនៃទិន្នន័យ។ ការការពារសុក្រឹតភាព រារាំងការផ្លាស់ប្តូរទិន្នន័យដែលគ្មានការអនុញ្ញាត។ វាធានាថាទិន្នន័យនៅតែត្រឹមត្រូវ មិនផ្លាស់ប្តូរ និង រក្សាទុក។

អនុវត្តន៍ការការពារសុក្រឹតភាពបានត្រឹមត្រូវ ផ្តល់នូវមធ្យោបាយប្រឆាំងនឹងសកម្មភាពដែលគ្មានការអនុញ្ញាតនិងព្យាបាទ ក៏ដូចជាអ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាត។

១.១.៣ លទ្ធភាព (Availability)

គោលការណ៍សំខាន់ទី៣នៃគោលការណ៍សន្តិសុខប្រព័ន្ធព័ត៌មានគឺលទ្ធភាព។ លទ្ធភាពគឺជាភាពមានសេវា ឬ ភាពដែលអាចប្រើប្រាស់បាន។ លទ្ធភាពមានន័យថា ប្រភព (source) ដែលមានការអនុញ្ញាត អាចធ្វើការអាក់សេសធនធាគ្រប់ពេលវេលានិងមិនមានការរំខាន។ ប្រសិនបើ

យន្តការសន្តិសុខផ្តល់នូវ «លទ្ធភាព» វាធានាថា ទិន្នន័យ វត្ថុ និងធនធានអាចធ្វើការអាក់សេសបានចំពោះអ្នកដែលមានការអនុញ្ញាត។

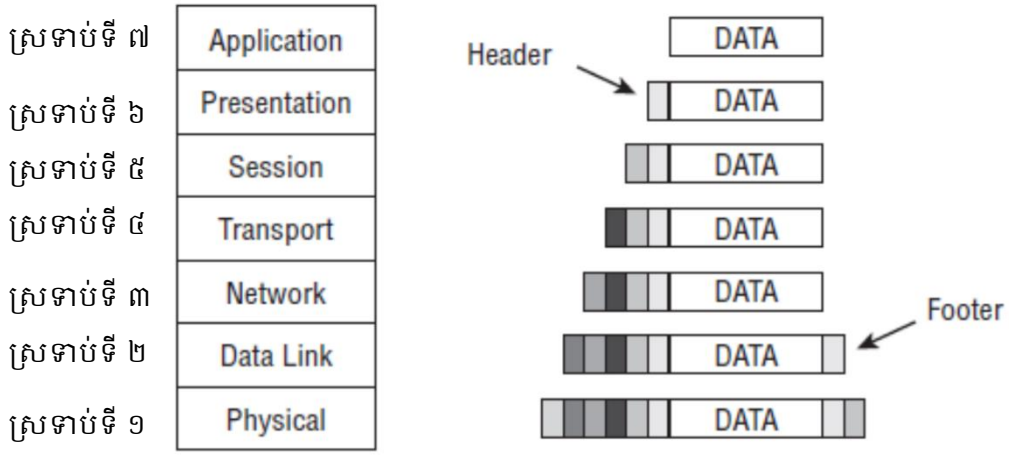
១.១.៤ មូលដ្ឋាននិងគោលការណ៍សន្តិសុខផ្សេងៗ (Others)

ក្រៅពីមូលដ្ឋានិងគោលការណ៍ទាំងបីនៃសន្តិសុខប្រព័ន្ធព័ត៌មានខាងលើ នៅមានមូលដ្ឋាននិងគោលការណ៍សន្តិសុខដទៃទៀតដូចជា ឯកជនភាព(Privacy) អត្តសញ្ញាណកម្ម (Identification) យថាភូតកម្ម(Authentication) អនុញ្ញាត(Authorization) សវនាការ(Auditing) គណនេយ្យភាព(Accountability) និង non-repudiation។

១.២ ម៉ូដែល OSI

គមនាគមន៍រវាងកុំព្យូទ័រលើបណ្តាញអាចធ្វើទៅបានដោយសារវិធីការ (Protocol)។ វិធីការគឺជាសំណុំក្បួនច្បាប់និងការរឹតត្បិតដែលកំណត់ពីរបៀបដែលទិន្នន័យត្រូវបានបញ្ជូនតាមមេឌាបណ្តាញ (Network Medium)។ នៅដំណាក់កាលដំបូងនៃការអភិវឌ្ឍន៍បណ្តាញ ក្រុមហ៊ុនជាច្រើនមានវិធីការរៀងៗខ្លួន ដែលមានន័យថា អន្តរកម្មរវាងកុំព្យូទ័ររបស់ក្រុមហ៊ុនផ្សេងៗគ្នាច្រើនតែមិនអាចទាក់ទងជាមួយគ្នាបាន។ ដើម្បីលុបបំបាត់បញ្ហានេះ អង្គការស្តង់ដាអន្តរជាតិ (ISO) បានបង្កើតម៉ូដែល OSI សម្រាប់វិធីការនានាឆ្នាំ១៩៨០ ។ ជាពិសេសOSI-៧៤៩៨ ត្រូវបានកំណត់ថាជាម៉ូដែល OSI។

ម៉ូដែល OSI បែងចែកភារកិច្ចបណ្តាញជាប្រាំពីរស្រទាប់ផ្សេងគ្នា។ ស្រទាប់នីមួយៗទទួលខុសត្រូវសម្រាប់អនុវត្តការងារជាក់លាក់ឬប្រតិបត្តិការសម្រាប់គមនាគមន៍រវាងកុំព្យូទ័រពីរ។ ស្រទាប់ទាំងនេះតែងតែរាប់ចាប់ពីក្រោមទៅលើ (សូមមើលរូបភាព ១១.១)។ ឧទាហរណ៍ស្រទាប់ទី៣ ត្រូវបានគេស្គាល់ថាជាស្រទាប់បណ្តាញ។ ស្រទាប់នីមួយៗទាក់ទងដោយផ្ទាល់ជាមួយស្រទាប់ខាងលើឬស្រទាប់ខាងក្រោមវា បូករួមនឹងស្រទាប់នៅលើប្រព័ន្ធដៃគូទំនាក់ទំនងរបស់វា។



Application	Data stream
Presentation	Data stream
Session	Data stream
Transport	Segment (TCP)/Datagram (UDP)
Network	Packet
Data Link	Frame
Physical	Bits

រូបភាពទី១៖ បង្ហាញពីស្រទាប់ OSI Model

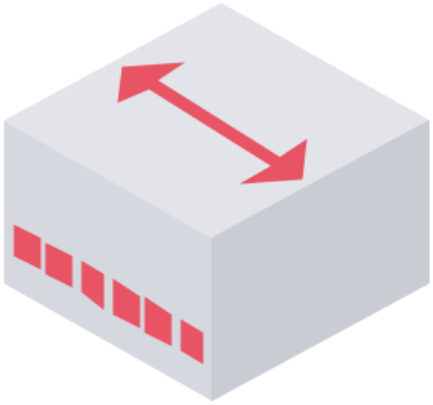
១.៣ ឧបករណ៍បណ្តាញ (Network Devices)

ដើម្បីបង្កើតបណ្តាញកុំព្យូទ័រមួយ យើងត្រូវការឧបករណ៍ជាច្រើន ដូចជាកុំព្យូទ័រ ទូរស័ព្ទឆ្លាតផ្ទោះពុម្ព។ ឧបករណ៍ដែលសំខាន់និងចាំបាច់សម្រាប់ភ្ជាប់ឧបករណ៍ដូចជា កុំព្យូទ័រ ទូរស័ព្ទឆ្លាតផ្ទោះពុម្ព ស្មែននន័យ ជាដើម ចូលគ្នាហៅថាឧបករណ៍បណ្តាញ។

១.៣.១ ឧបករណ៍ Hub

Hub ជាចំណុចតំណរួមមួយសម្រាប់ភ្ជាប់គ្រប់ឧបករណ៍ក្នុងបណ្តាញ។ Hub ភ្ជាប់អង្កត់លែន (LAN Segment) ចូលគ្នា មានច្រើនច្រក (Ports) និង ធ្វើការនៅស្រទាប់ទី១នៃម៉ូដែល OSI។ ពេលដុំទិន្នន័យមួយមកដល់ច្រកមួយ វាចម្លងទៅគ្រប់ច្រកទាំងអស់ ដើម្បីឱ្យអង្កត់នៃលែនទាំង

អស់អាចមើលឃើញដុំទិន្នន័យនោះ។ វាបញ្ជូនដុំនោះទៅគ្រប់ច្រកទាំងអស់ ដោយពឹងផ្អែកលើព័ត៌មាននៅស្រទាប់ទី១ (ប៊ីតឬសញ្ញា) ។ ការបញ្ជូននេះបណ្តាលឱ្យមានដែនប៉ះទង្គិចធំ (Collision Domain) និង ដែនផ្សព្វផ្សាយធំ (Broadcast domain) ក្នុងបណ្តាញ។ ច្រកនីមួយៗនៃ Hub មានល្បឿនកំណត់មួយដែលអាស្រ័យទៅលើល្បឿនសរុប។ ល្បឿនច្រកនីមួយៗស្មើនឹងល្បឿនសរុបចែកនឹងចំនួនច្រកនៃ Hub។



រូបភាពទី២៖ បង្ហាញពីឧបករណ៍ Hub

១.៣.២ ឧបករណ៍ Layer 2 Switch

ជួនកាល Switch ហៅថា Bridge ដែលជាធម្មតាអាចមានត្រឹមតែពីរច្រក។ Switch អាចមានច្រើនច្រក(Port) ដែលអាស្រ័យទៅលើថាតើគេត្រូវភ្ជាប់ទៅអង្កត់នៃលេនចំនួនប៉ុន្មាន។ ពេលដុំទិន្នន័យមួយមកដល់ច្រកមួយ វាចម្លងទៅត្រឹមតែច្រកគោលដៅមួយប៉ុណ្ណោះ។ ក្នុងករណីខ្លះ វាអាចចម្លងទៅគ្រប់ច្រក កាលណាមេម៉ូរីនៃ Content Address Memory (CAM) របស់វាពេញ។ វាបញ្ជូនទិន្នន័យពឹងផ្អែកលើព័ត៌មាននៅស្រទាប់ទី២នៃម៉ូដែល OSI។ ពេលគឺប្រើអាសយដ្ឋានម៉ែក (MAC address) នៃឧបករណ៍ទាំងអស់ដែលភ្ជាប់មកវាសម្រាប់បញ្ជូនទៅគោលដៅ។ ការបញ្ជូននេះបណ្តាលឱ្យមានដែនផ្សាយធំដូច Hub ដែរ ប៉ុន្តែដែនប៉ះទង្គិចតូច (បើ Switch មានច្រកបញ្ជូន ៤ ដែនប៉ះទង្គិចមានត្រឹមតែ ៤ ដែរ)។ ច្រកនីមួយៗនៃ Switch មានល្បឿនជាក់លាក់ដែលអាស្រ័យទៅលើល្បឿនសរុប។ ល្បឿនច្រកបញ្ជូននីមួយៗស្មើនឹងល្បឿនសរុបនៃ Switch។

រូបភាពទី៣៖ បង្ហាញពីឧបករណ៍ Switch

១.៣.៣ ឧបករណ៍ Bridge

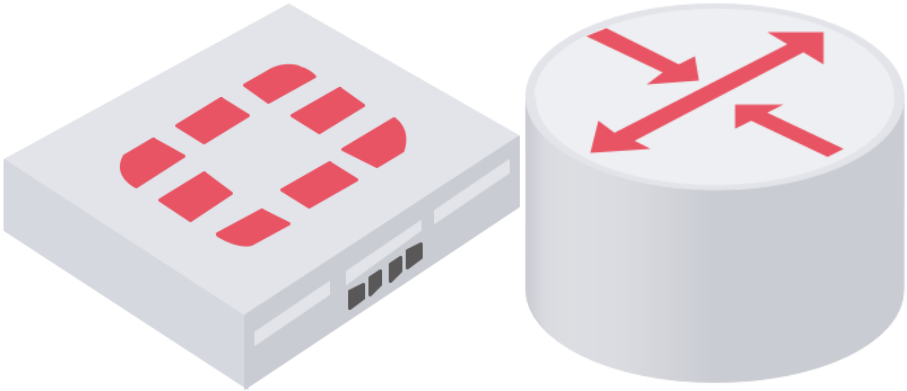
Bridge ត្រូវគេចាត់ទុកជា Layer 2 Switch។ វាឧបករណ៍ដំណើរការនៅស្រទាប់ទី២នៃម៉ូដែល OSI ហើយគេរៀបចំឡើងដើម្បីភ្ជាប់លៃនឬអង្កត់លៃន (LAN/LAN Segment) ពីរឬច្រើនចូលគ្នា ដែលនីមួយៗមានដែនប៉ះទង្គិចផ្សេងៗគ្នា ឬ ដើម្បីញែកបណ្តាញមួយទៅជាបណ្តាញច្រើន។ ជាទូទៅ បណ្តាញទាំងអស់ដែលភ្ជាប់ទៅ Bridge ត្រូវប្រើវិធីការដូចគ្នា ពោលគឺបើប្រើបច្ចេកវិទ្យាលៃន Ethernet ត្រូវប្រើ Ethernet ទាំងអស់ បើប្រើ AppleTalk ត្រូវប្រើ AppleTalk ទាំងអស់។ មុខងារចំបងនៃ Bridge គឺការបញ្ជូនទិន្នន័យ ដោយពឹងផ្អែកលើអាសយដ្ឋានម៉ាក់របស់ឧបករណ៍បញ្ជូនឬទទួល។

រូបភាពទី៤៖ បង្ហាញពីឧបករណ៍ Bridge

១.៣.៤. **ឧបករណ៍** Router

Router ជាប្រភេទឧបករណ៍អន្តរបណ្តាញដែលធ្វើការនៅស្រទាប់ទី៣នៃម៉ូដែល OSI និងដែលនាំទិន្នន័យផ្សេងៗគ្នាឆ្លងកាត់អន្តរបណ្តាញ ដោយពឹងផ្អែកលើអាសយដ្ឋានអាយភី (IP address) អាសយដ្ឋាន បណ្តាញ (Network address)។ Router អាចសម្រេចស្វែងរកផ្លូវប្រសើរ និងជិតបំផុត សម្រាប់ចែកចាយទិន្នន័យលើបណ្តាញ។ តាមច្បាប់ Router មិនបញ្ជូនដែនផ្សាយពីបណ្តាញមួយទៅបណ្តាញមួយទៀតទេ។ មានន័យថាពេល Switch ឬ Hub បង្កើតដែនផ្សាយហើយពេលជួបនឹង Router ដែនផ្សាយទាំងនោះនឹងត្រូវបញ្ចប់។ តែវាក៏ខណ្ឌដែនផ្សាយដែរ។ ចំណែកដែនប៉ះទង្គិចមានលក្ខណៈដូច Switch ដែរ។

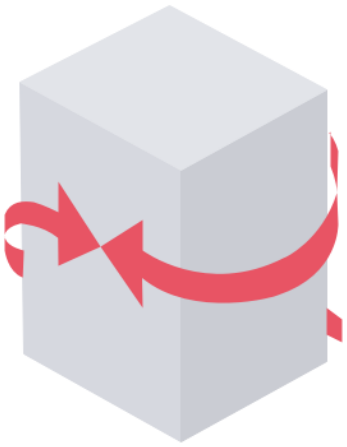
សូមចងចាំថា Switch ខណ្ឌដែនប៉ះទង្គិច ចំណែកឯ Router ខណ្ឌដែនផ្សាយ។



រូបភាពទី៥៖ បង្ហាញពីឧបករណ៍ Routers

១.៣.៥ **ច្រកបណ្តាញ** (Gateway)

ច្រកបណ្តាញ (Gateway) ជាឧបករណ៍បំប្លែងវិធីការ (Protocol Converter) និងដំណើរការនៅស្រទាប់ទី៣នៃម៉ូដែល OSI តែទោះជាយ៉ាងណាក៏ដោយ អាស្រ័យតាមមុខងារ ច្រកបណ្តាញក៏ធ្វើការនៅស្រទាប់ផ្សេងៗនៃម៉ូដែល OSI ផងដែរ ដូចជាស្រទាប់ទី៧ ទី ៥ ទី៤។ Router ខ្លួនឯងបំប្លែង ទទួល និង បញ្ជូនបន្តដុំទិន្នន័យកាត់ត្រឹមតែបណ្តាញដែលប្រើវិធីការដូចគ្នា។ ផ្ទុយមកវិញច្រកបណ្តាញអាចទទួលយកដុំទិន្នន័យពីវិធីការមួយ និងបំប្លែងវាទៅជាដុំទិន្នន័យសម្រាប់វិធីការមួយផ្សេងទៀត មុននឹងរុញចេញ។ ច្រកបណ្តាញគឺជា Router។



រូបភាពទី៦៖ បង្ហាញពីឧបករណ៍ Gateway

១.៣.៦ ចំណុចអាក់សេស/អាក់សេសភ័ញ្ជ (Access Point/Wireless AP)

ចំណុចអាក់សេសឬអាក់សេសភ័ញ្ជគឺជាឧបករណ៍ដែលធ្វើការជាពូរ (core) នៃបណ្តាញឥតខ្សែ សម្រាប់ភ្ជាប់ឧបករណ៍វ៉ាយហ្វាយទៅបណ្តាញកុំព្យូទ័រ។

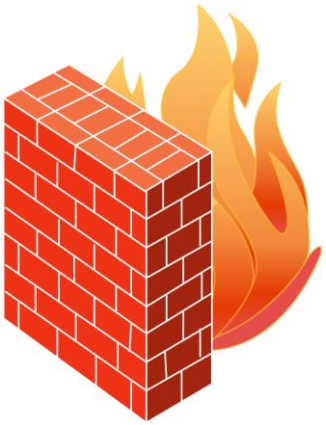
រូបភាពទី៧៖ បង្ហាញពីឧបករណ៍ Wireless Access Point

១.៤. ការការពារបណ្តាញ (Network Defense)

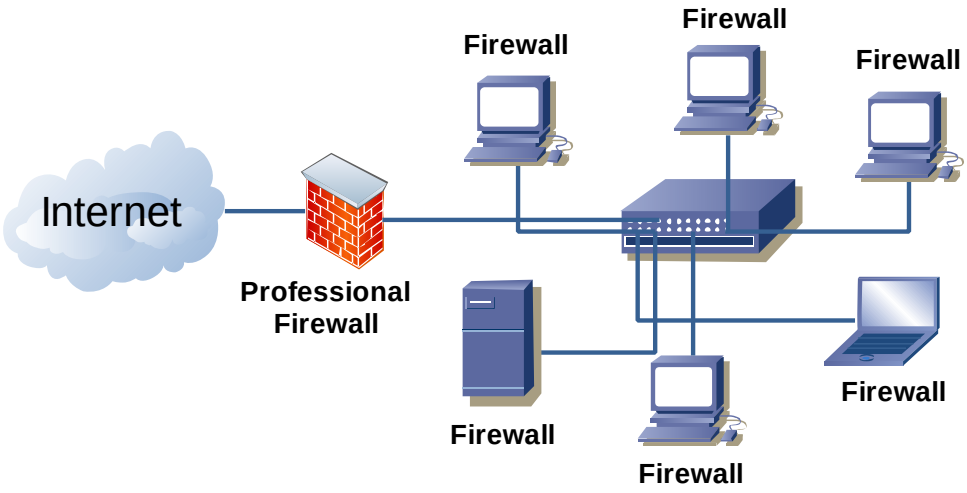
ការប្រើប្រាស់ឧបករណ៍និងដំណោះស្រាយដ៏ត្រឹមត្រូវអាចជួយការពារបណ្តាញរបស់យើងបានប្រសើរ។ ឧបករណ៍ការពារបណ្តាញមានច្រើនប្រភេទ និងអាចការពារតាមតួនាទីរបស់វា។ យើងអាចប្រើឧបករណ៍ទាំងនេះជាខ្សែការពារទី១ ទី២ ទី៣ ទី៤ និងខ្សែការពារចុងក្រោយ នៃបណ្តាញកុំព្យូទ័ររបស់យើង។ យ៉ាងតិចណាស់ យើងត្រូវរៀបចំខ្សែការពារជាច្រើនចូលគ្នា ផ្ទុយមកវិញ មានខ្សែការពារបណ្តាញតែមួយ មិនអាចការពារបណ្តាញបានទេ។

១.៤.១ ជញ្ជាំងភ្លើង (Firewall)

ជញ្ជាំងភ្លើងគឺជាប្រព័ន្ធសុវត្ថិភាព (ហាដវែរឬសុសវែរ) ដែលត្រួតពិនិត្យលំហូរទិន្នន័យពីកុំព្យូទ័រមួយទៅកុំព្យូទ័រមួយទៀត ឬពីបណ្តាញកុំព្យូទ័រមួយទៅបណ្តាញកុំព្យូទ័រមួយទៀតឬពីអ៊ីនធឺណិត ប្រឆាំងនឹងអាក់សេសខុសច្បាប់ពីខាងក្រៅ ឬ ប្រឆាំងនឹងការខូចហាដវែរនៅកន្លែងណាមួយនៃបណ្តាញ។ គោលបំណងសំខាន់នៃជញ្ជាំងភ្លើងគឺបិទចរាចរទិន្នន័យពីខាងក្រៅ ប៉ុន្តែក៏អាចបិទចរាចរទិន្នន័យពីខាងក្នុងបានដែរ។ ជញ្ជាំងភ្លើងជាយន្តការការពារជួរមុខទីមួយប្រឆាំងនឹងល្បួចណាមួយ។ ជញ្ជាំងភ្លើងអាចជាហាដវែរដែលសង់នៅក្នុងឧបករណ៍ដូចជា Router ដែលត្រូវការរៀបចំបន្ថែមទៀតដើម្បីឱ្យមានប្រសិទ្ធភាព និង ដែលប្រើបច្ចេកទេស Packet-Filter។ ហើយវាក៏អាចជាសុសវែរពេញនិយមបំផុតដែលអាចការពារបណ្តាញសម្រាប់អ្នកប្រើប្រាស់តាមផ្ទះ ដែលអាចប្រឆាំងនឹងមេរោគផងដែរ និង ដែលត្រូវការអាប់ដេតជាប្រចាំ។ ជញ្ជាំងភ្លើងអាចជាបន្សំទាំងពីរប្រភេទចូលគ្នា ហើយជញ្ជាំងភ្លើងតាំងនៅចន្លោះបណ្តាញខាងក្នុង ដូចជា សែន លែន មែន ឬ វែន និង បណ្តាញខាងក្រៅ ដូចជាអុីនធឺណិត ដើម្បីការពារបណ្តាញខាងក្នុង។



រូបភាពទី៨៖ បង្ហាញពីជញ្ជាំងភ្លើងឬ Firewall



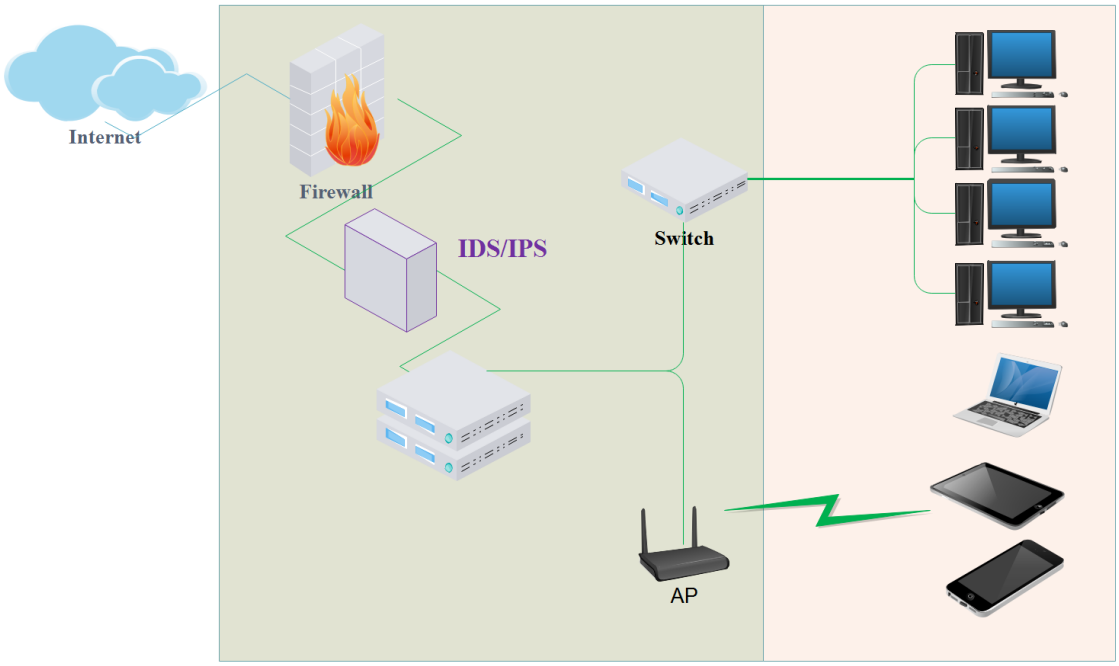
រូបភាពទី៩៖ បង្ហាញពីការតប្រព័ន្ធបណ្តាញ

១.៤.២ ប្រព័ន្ធអង្កេតល្មួច (Intrusion Detection System)

ប្រព័ន្ធអង្កេតល្មួចគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់ប្រមូលផ្តុំ អង្កេតវិភាគព័តមាន និង ត្រួតពិនិត្យរាល់សកម្មភាពក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ ដើម្បីកំណត់អត្តសញ្ញាណរង្វាយប្រហារឬសកម្មភាពល្មួច ក្នុងគោលបំណងការពារ ភាពសម្ងាត់(Confidentiality) សុក្រឹតភាព(Integrity) លទ្ធភាព (Availability) និង គណនេយ្យភាព(Accountability)។

បច្ចុប្បន្ន មានបច្ចេកវិទ្យាថ្មីមួយទៀតដែលអាចចាត់ទុកថាជាបច្ចេកវិទ្យាជំនាន់ទី២នៃប្រព័ន្ធអង្កេតល្មួចគឺ ប្រព័ន្ធអង្កេតវិវាទ(Breach Detection System)។

ប្រព័ន្ធអង្កេតវិវាធគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត និង ត្រួតពិនិត្យ សកម្មភាពម៉ាល់វែរ កិច្ចកំហែងផ្សេងៗ ក្រោយពេលមានវិវាទកើតឡើងក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ។



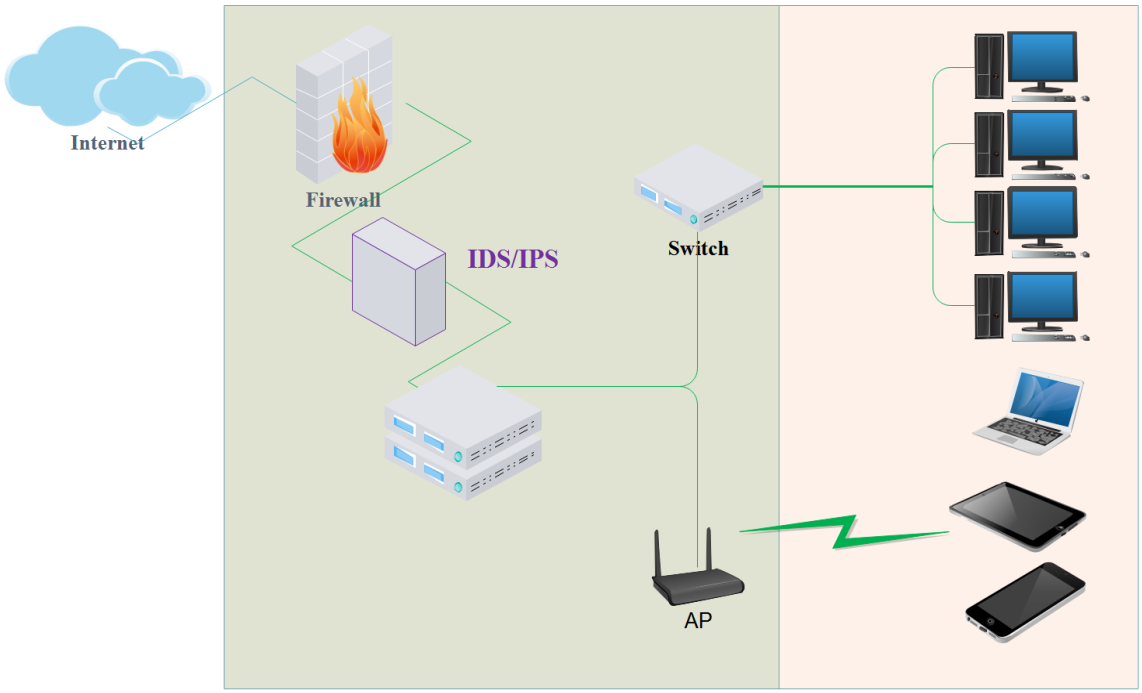
រូបភាពទី១០៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បីអង្កេតពីការជ្រៀតចូលនៃ Viruses

១.៤.៣ ប្រព័ន្ធបង្ការល្ងួច (Intrusion Prevention System)

ប្រព័ន្ធបង្ការល្ងួចគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត បង្ការ ត្រួតពិនិត្យអាក់សេសឬសកម្មភាពក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ និង ចាត់វិធានឆុតកាល (real-time) ទៅនឹងសកម្មភាពនោះ ដើម្បីការពារអង្វាយប្រហារ ការបំពាន ឬ សកម្មភាពលួច។ ជាទូទៅគេប្រើប្រាស់វាជាមួយប្រព័ន្ធអង្កេតល្ងួច។

ដូចគ្នាទៅនឹងប្រព័ន្ធអង្កេតល្ងួចដែរ មានបច្ចេកវិទ្យាចុងក្រោយដែលជាបច្ចេកវិទ្យាជំនាន់ទី២ នៃប្រព័ន្ធបង្ការល្ងួចគឺប្រព័ន្ធបង្ការរវិាទ (Breach Prevention System)។

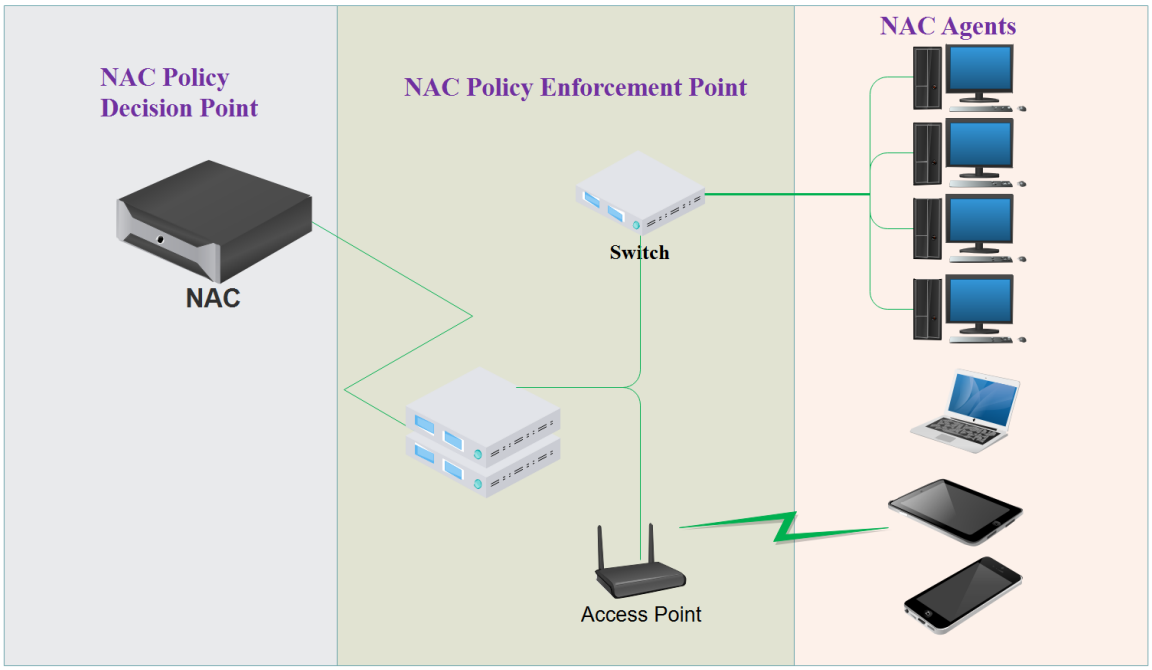
ប្រព័ន្ធបង្ការរវិាទគឺជាហាដវែរឬសុសវែរមួយប្រភេទដែលរចនាឡើងសម្រាប់អង្កេត បង្ការ រវិាគសកម្មភាពម៉ាល់វែរ កិច្ចកំហែងផ្សេងៗ និង ចាត់វិធានការឆុតកាល (real-time) មុនពេលរវិាទ កើតឡើងក្នុងកុំព្យូទ័រឬបណ្តាញកុំព្យូទ័រ។



រូបភាពទី១១៖ បង្ហាញពីការរៀបចំប្រព័ន្ធដើម្បីបង្ការពីការជ្រៀតចូលនៃ Viruses

១.៤.៤ ប្រព័ន្ធត្រួតអាក់សេសបណ្តាញ (Network Access Control System/NAC)

ប្រព័ន្ធត្រួតអាក់សេសបណ្តាញ គឺជាបច្ចេកវិទ្យា វិធីសាស្ត្រ ឬ ដំណោះស្រាយដែលអនុវត្ត ដោយបង្ខំនូវគោលនយោបាយសន្តិសុខប្រព័ន្ធព័ត៌មានសម្រាប់កំណត់ បែងចែក ចាត់ចែងសិទ្ធិ គ្រប់គ្រង ដោយស្វ័យប្រវត្តលើឧបករណ៍ទាំងអស់ដែលចូលអាក់សេសបណ្តាញ ដើម្បីធានា បង្កើននិងជំរុញ ការពារសន្តិសុខបណ្តាញ ហើយនិង កាត់បន្ថយហានិភ័យ។



រូបភាពទី១២៖ បង្ហាញពីប្រព័ន្ធ Network Access Control System

១.៤.៥ ចម្រោះវេប (Web Filter)

ចម្រោះវេបជាបច្ចេកវិទ្យា កម្មវិធី ឬលក្ខណៈមួយដែលអាចរឹងទំព័រវេបឬខ្លឹមសារនៃទំព័រវេប អំឡុងពេលប្រើប្រាស់ធ្វើអាក់សេសទំព័រវេប។

១.៤.៦ សេវ្ឌបករណ៍ Proxy (Proxy Server)

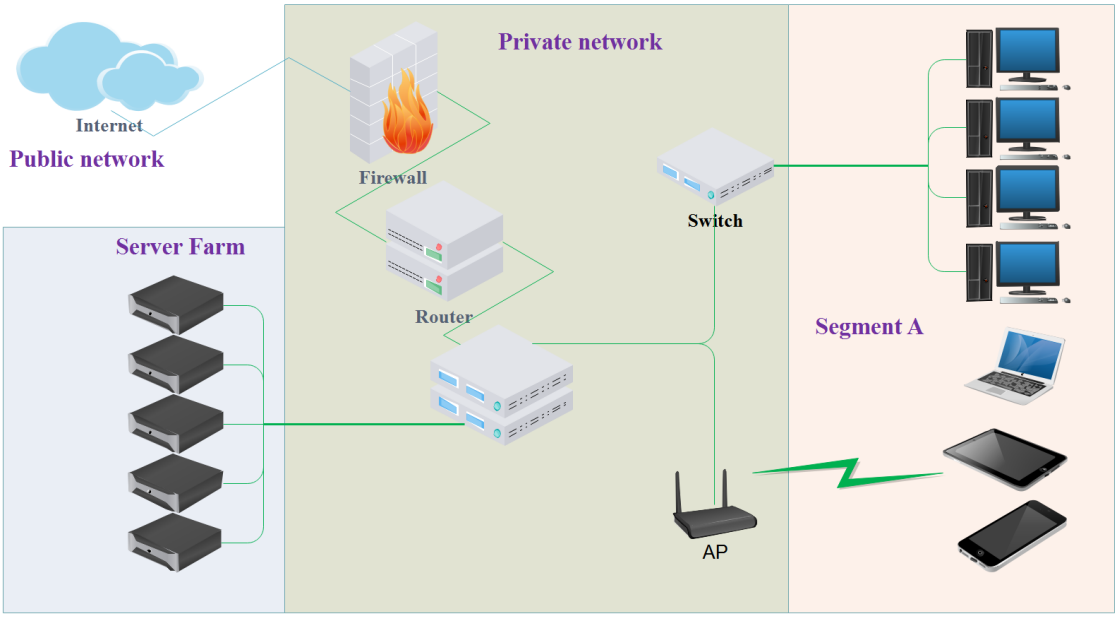
សេវ្ឌបករណ៍ Proxy ជាសេវ្ឌបករណ៍ទាំងឡាយណាដែលដើរតួជាអន្តរការីចំពោះសំណើរបស់អតិថិជនទៅសេវ្ឌបករណ៍ពិត សម្រាប់សេវាឬធនធាន។ មានសេវ្ឌបករណ៍ Proxy ជាច្រើនប្រភេទដែលអាចប្រើបានអាស្រ័យលើគោលបំណងផ្សេងៗ។ សេវ្ឌបករណ៍ Proxy អាចការពារបានត្រឹមតែកម្មវិធីទាំងឡាយណាដែលគាំទ្រវា។

១.៤.៧ អង់ទីម៉ាល់វែរ (Anti-malware)

វាជាសុសវែរម្យ៉ាងដែលបង្កើតឡើងដើម្បីប្រឆាំង រារាំង ការពារ អង្កេត និងលុបបំបាត់ម៉ាល់វែរនៅក្នុងកុំព្យូទ័រ ប្រព័ន្ធបច្ចេកវិទ្យាព័ត៌មាន ឬ ឧបករណ៍កុំព្យូធីង(Computing devices)។ ម៉ាល់វែរជាសុសវែរឬកូដសុសវែរ ដែលបង្កើតឡើងក្នុងគោលបំណងមិនល្អណាមួយនិងមានសមត្ថភាពបំផ្លាញឯកសារប្រព័ន្ធកុំព្យូទ័រ ...។ ឧ. មេរោគកុំព្យូទ័រជាកម្មវិធីប្រភេទម៉ាល់វែរ។

១.៥ ប្រភេទអង្គត់បណ្តាញ (Network Segment Types)

អង្គត់បណ្តាញគឺជាផ្នែកមួយនៃបណ្តាញកុំព្យូទ័រដែលត្រូវបានបំបែកចេញពីបណ្តាញមួយ ដោយឧបករណ៍ដូចជា Hub, Bridge, Switch និង Router ។ ផ្នែកនីមួយៗអាចមានកុំព្យូទ័រមួយឬច្រើនឬឧបករណ៍ផ្សេងទៀត។



រូបភាពទី១៣៖ បង្ហាញពី Network Segment Types

១.៥.១ បណ្តាញសាធារណៈ (Public Network)

បណ្តាញសាធារណៈ:គឺជាបណ្តាញមួយប្រភេទ ដែលជនទូទៅអាចចូលប្រើបាន និង អាចភ្ជាប់ទៅបណ្តាញផ្សេងទៀតឬអ៊ីនធឺរណិត។ បណ្តាញនេះផ្ទុយពីបណ្តាញឯកជនដែលការពិតបន្តឹងនិងច្បាប់ប្រើប្រាស់ ត្រូវបានបង្កើតឡើងដើម្បីកាត់បន្ថយការចូលប្រើ។ ពេលធ្វើការអាក់សេសបណ្តាញសាធារណៈ អ្នកប្រើប្រាស់ត្រូវស្វ័យប្រុងប្រយ័ន្ធចំពោះហានិភ័យ។

១.៥.២ បណ្តាញឯកជន (Private Network)

បណ្តាញឯកជនគឺជាបណ្តាញកុំព្យូទ័រមួយដែលប្រើអាសយដ្ឋានអាយភីឯកជន (private IP address)។ ស្តង់ដ (Specification)ទាំង IPv4 និង IPv6 បានកំណត់នូវប្រវែងអាសយដ្ឋានអាយភីឯកជន។ អាសយដ្ឋានទាំងនេះត្រូវបានប្រើជាទូទៅសម្រាប់បណ្តាញក្នុងតំបន់ (លែន) នៅក្នុង

តំបន់លំនៅដ្ឋាន ការិយាល័យ និង សហគ្រាស។ បណ្តាញឯកជនមានការរឹតបន្តឹងនិងច្បាប់ប្រើប្រាស់ដើម្បីកាត់បន្ថយការចូលប្រើ ហានិភ័យលើសន្តិសុខ។

១.៥.៣ បណ្តាញកូនកាត់ (semi-public Network)

បណ្តាញសាធារណៈនិងបណ្តាញឯកជនផ្គុំចូលគ្នាបង្កើតបានជាបណ្តាញពាក់កណ្តាលសាធារណៈ។ ជាធម្មតា វាជាបណ្តាញដែលអ្នកប្រើប្រាស់អាចធ្វើការអាក់សេសទៅបណ្តាញសាធារណៈ។

១.៥.៤. បណ្តាញតំបន់ស (Demilitarized Zone-DMZ)

បណ្តាញតំបន់សជាបណ្តាញរងមួយរបស់ស្តាប័នសម្រាប់ភ្ជាប់កុំព្យូទ័រឬឧបករណ៍ (host) ដែលត្រូវការអាក់សេសទៅបណ្តាញខាងក្រៅ ពោលគឺទៅអ៊ីនធឺណិត ឧទាហរណ៍៖ សេវ៉ូបករណ៍វេប (Web servers)។ DMZ អាចជាបណ្តាញសមស្របសម្រាប់ដោះស្រាយជាមួយរង្វាយប្រហារខាងក្រៅ ហើយអាចត្រូវបានប្រើដើម្បីអនុវត្តគោលនយោបាយគ្រប់គ្រងអ្នកប្រើខាង ក្នុងប៉ុន្តែមានការប្រើតិចតួចប្រឆាំងនឹងរង្វាយប្រហារខាងក្នុង។

ជំពូកទី២

ផែនការអនុវត្តន៍គម្រោង

ផែនការសកម្មភាពជាចំណុចសំខាន់នៃការសម្រេចគម្រោង។ ខាងក្រោមជាផែនការអនុវត្តន៍នៃគម្រោងនៃប្រព័ន្ធបណ្តាញណែតវឺក។

២.១ បរិយាយទូទៅនៃគម្រោង

ដើម្បីបង្កើតប្រព័ន្ធនៃការសិក្សាស្រាវជ្រាវនេះឱ្យទទួលបានជោគជ័យតាមការរំពឹងទុក អ្នកអនុវត្តគម្រោងត្រូវរៀបចំវិធីសាស្ត្រឱ្យបានច្បាស់លាស់ ដូចខាងក្រោមជាដំណាក់កាលនៃការរៀបចំ៖

ទី១៖ កំណត់បញ្ហានិងគោលបំណង

ទី២៖ ប្រមូលព័ត៌មាននិងឯកសារសម្រាប់តម្រូវការគម្រោង

ទី៣៖ វិភាគតម្រូវការប្រព័ន្ធ និង រៀបចំរចនាប្រព័ន្ធ

ទី៤៖ ដំឡើង បង្កុំ និងពិសោធ

ទី៥៖ រៀបចំនិងក្រងឯកសារ

២.២ ផែនការកាលវិភាគនិងតារកិច្ច

ខាងក្រោមជាបំណែងចែកពេលវេលានិងភារកិច្ចអ្នកទទួលខុសត្រូវ។

ល.រ	ផែនការ	ពេលវេលា	ភារកិច្ច
១	កំណត់ពីបញ្ហានិងគោលបំណង	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
២	ប្រមូលព័ត៌មានឯកសារសម្រាប់តម្រូវការគម្រោង	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
៣	វិភាគតម្រូវការប្រព័ន្ធ និង រៀបចំរចនាប្រព័ន្ធ	២សប្តាហ៍	គង់ រក្សា សន សំខាន់
៤	ដំឡើង បង្កុំ និងពិសោធ	២សប្តាហ៍	គង់រក្សា សន សំខាន់
៥	រៀបចំនិងក្រងឯកសារ	៣សប្តាហ៍	គង់ រក្សា សន សំខាន់

២.៣ លក្ខខណ្ឌនិងតម្រូវការសម្ភារៈ (Security Testing)

គម្រោងនៃការរៀបចំប្រព័ន្ធនេះត្រូវការសម្ភារៈនិងលក្ខខណ្ឌមួយចំនួន។លក្ខខណ្ឌនិងសម្ភារៈទាំងនៅរួមមាន៖

- Router: TP-LINK Wireless N Router TL-WR940N
- Wireless Access Point៖ TP-LINK Wireless N Router TL-WR940N
- កុំព្យូទ័រ៖ CPU: Core i7 8Gen, RAM: 8GB , SSD: 500GB, Graphic Card: GTX-1050 TI 4GB, HDD: 1TB,
- កម្មវិធី: Nmap, Nessus,

២-៤. លទ្ធផលរំពឹងទុក

ក្នុងពេលការសិក្សាពីគម្រោង ក្រុមរបស់ពួកយើងបានរំពឹងទុកចំនួនពីលទ្ធផលចំនួន ៣ធំៗ៖

១.ពួកយើងរំពឹងទុកថាវាអាចជួយ ការពារប្រព័ន្ធបណ្តាញរបស់អ្នកពីការជ្រៀតចូលនៃ Virus នឹងងាយស្រួលក្នុងការគ្រប់គ្រង

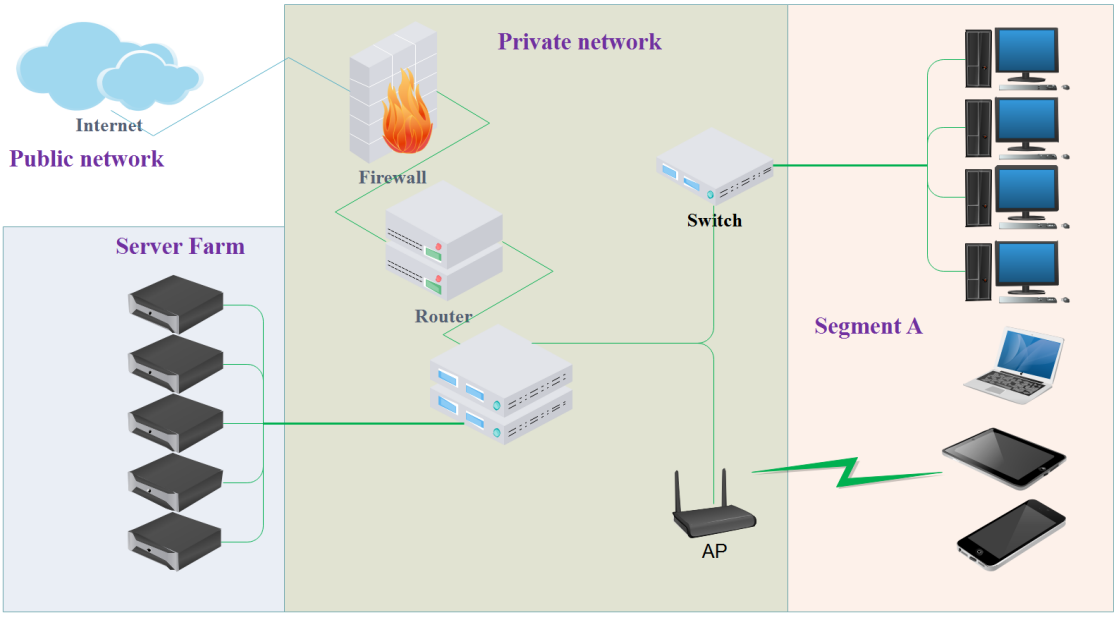
២.ការពង្រឹងទៅលើសន្តិសុខរបស់ Wireless Router ដូចជាការបើកដំណើរការ Firewall, Web Filter and Access Control

៣. ការពារទៅលើ End-Devices ដែលប្រើប្រាស់ដើម្បី Access ចូលទៅកាន់ Router ដូចជាការប្រើប្រាស់កម្មវិធីជំនួយ នឹងបើកដំណើរការប្រព័ន្ធសន្តិសុខដែលមានស្រាប់នៅលើវា

ជំពូកទី៣

ជំនឿចនិងបង្កុំសន្តិសុខបណ្តាញ

ជំពូកនេះ យើងបរិយាយអំពីវិធីសាស្ត្រនៃការសិក្សាស្រាវជ្រាវ។ វិធីសាស្ត្រស្រាវជ្រាវរបស់យើងគឺជំឡើងនិងបង្កុំសន្តិសុខបណ្តាញកុំព្យូទ័រកម្រិតតូចដែលមានរចនាសម្ព័ន្ធដូចខាងក្រោម៖



រូបភាពទី ១៤ ៖ បង្ហាញពីដ្យាក្រាមនៃបណ្តាញសន្តិសុខ Network

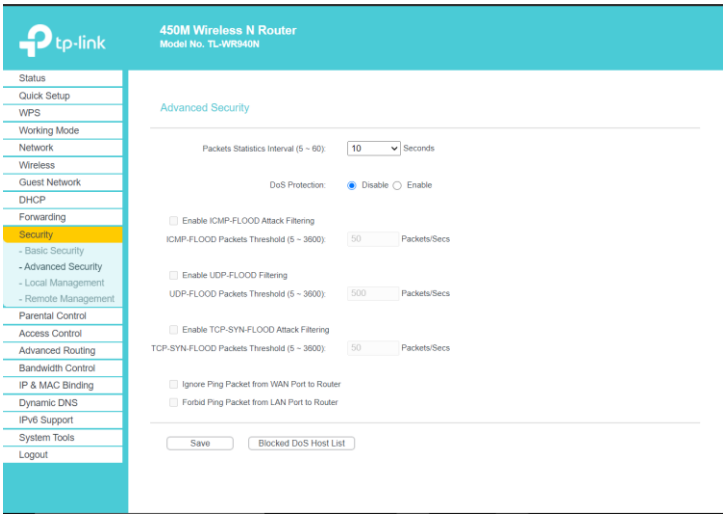
៣.១ សន្តិសុខបណ្តាញ (Network Security)

៣.១.១ របៀបនៃការដំណើរជញ្ជាំងភ្លើង (Firewall)

ដើម្បីឲ្យណែតវឺកយើងមានសុវត្ថិភាពយើងត្រូវ តំឡើងជញ្ជាំងភ្លើង នឹងកំណត់ជញ្ជាំងភ្លើងដូចខាងក្រោម៖

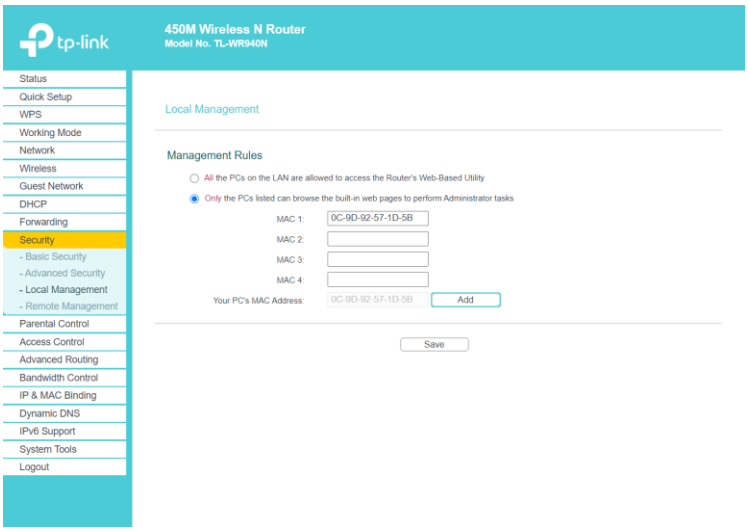
១.ចូលទៅកាន់ Console Screen របស់ Router ហើយរកមើលពាក្យថា Security-> Basic Security អ្នកនឹងបានឃើញ ពាក្យថា Firewall ចុច ពាក្យថា Enable ហើយចុច Save៖

២.បន្ទាប់ពីចុច Enable Firewall រួចហើយ សូមចូលទៅកាន់ពាក្យថា Advanced Security -> Enable Dos Protection-> ចុច check នៅត្រង់ Ignore Ping Packet from WAN Port to Router->Save៖



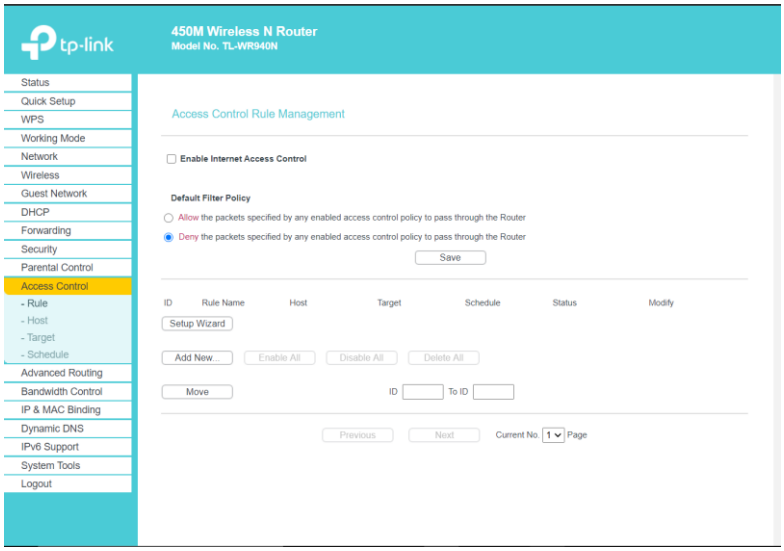
រូបភាពទី ១៥ ៖ បង្ហាញពីការបើក Firewall

៣.បន្ទាប់មកចូលទៅកាន់ Local Management ជ្រើសរើសយក Only ហើយចុចពាក្យថា Add អ្នកនឹងបានឃើញ Mac Address បង្ហាញឡើង បន្ទាប់មក Save៖



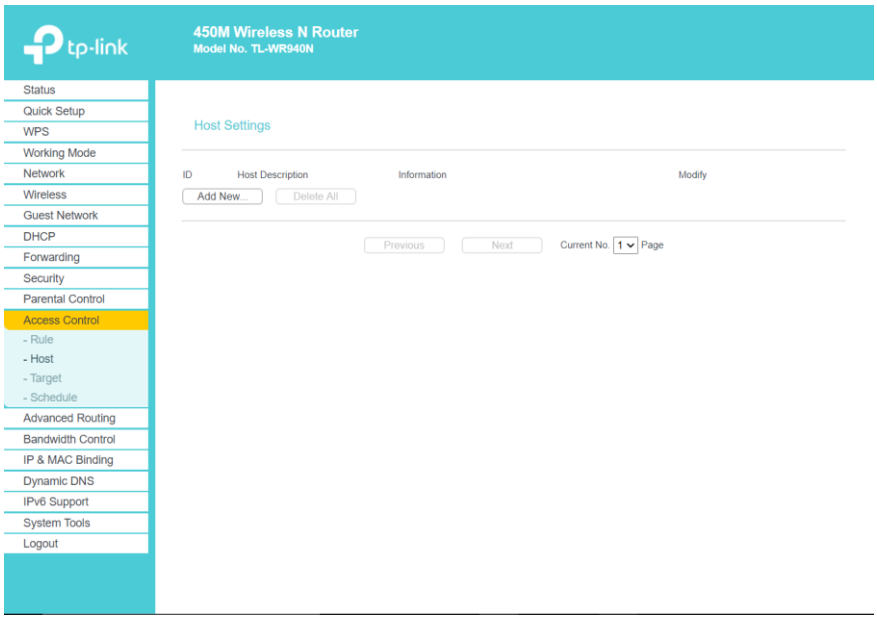
រូបភាពទី ១៦ ៖ បង្ហាញពីការការកំណត់ទៅលើ Local Management លើ Firewall

៤.បន្ទាប់មកចូលទៅកាន់ Access Control ចុចពាក្យថា Deny ហើយចុច Save៖

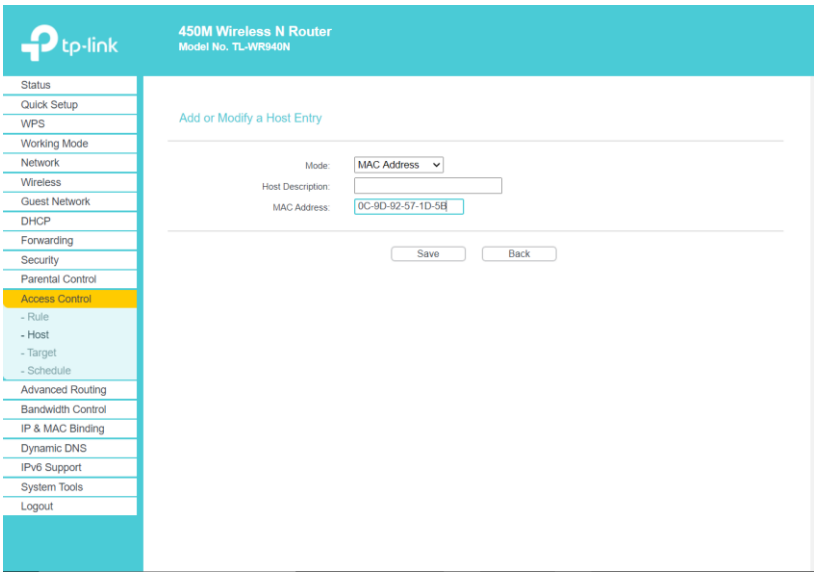


រូបភាពទី ១៧ ៖ បង្ហាញពីការបើកដំណើរការលើ Access Control

៥.ចូលមកកាន់ Host -> Add New -> ទៅ Copy Mac Address ពី Local Management ហើយបន្ទាប់មកយើងចុច Save៖

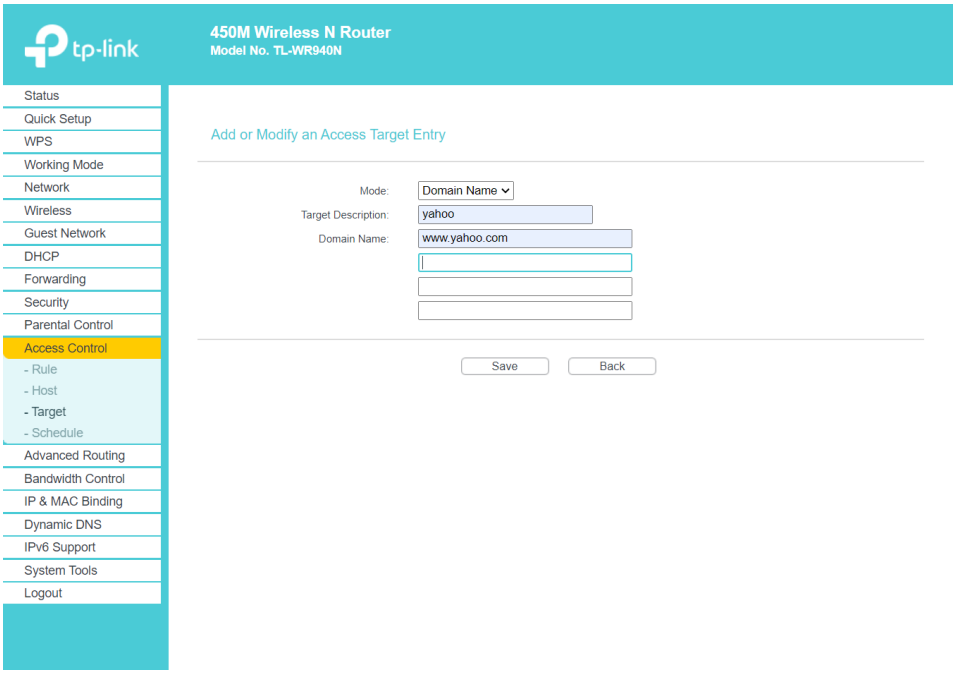


រូបភាពទី ១៨ ៖ បង្ហាញពីការ Add New Host នៅលើ Access Control



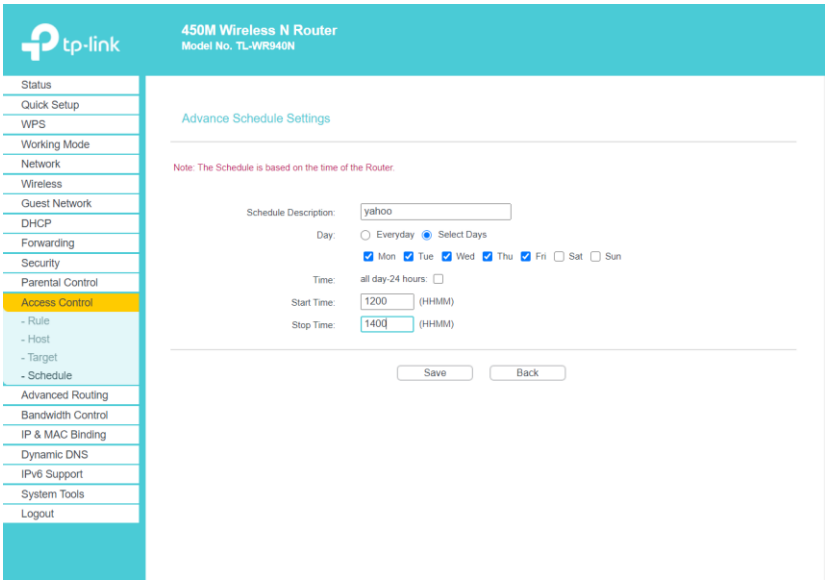
រូបភាពទី ១៩ ៖ បង្ហាញពី Mac Address នៅលើ Access Control

៦.ចូលមកកាន់ Target ហើយបំពេញពិត៌មានដែលមាន ដូចខាងក្រោម ហើយបន្ទាប់មក ចុច Save៖



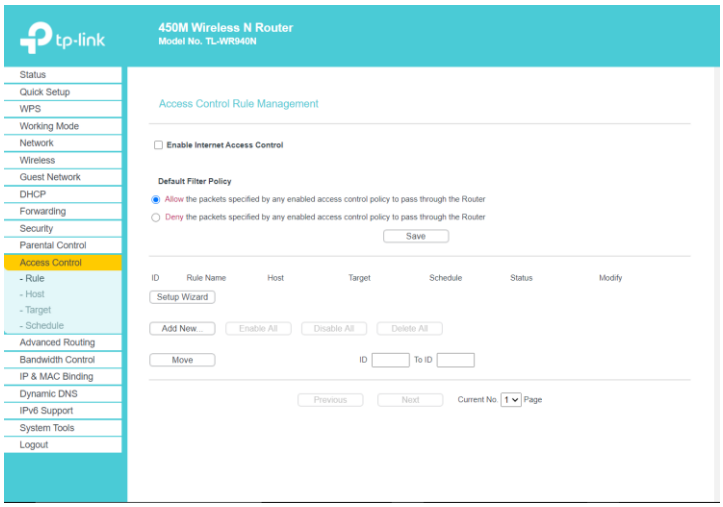
រូបភាពទី ២០ ៖ បង្ហាញពីការកណត់ទៅលើ Target នៅលើ Access Control

៧.បន្ទាប់មកចូលមកកាន់ Schedule ហើយធ្វើការបំពេញពិត័មានដូចខាងក្រោម ហើយសូមចុច Save៖

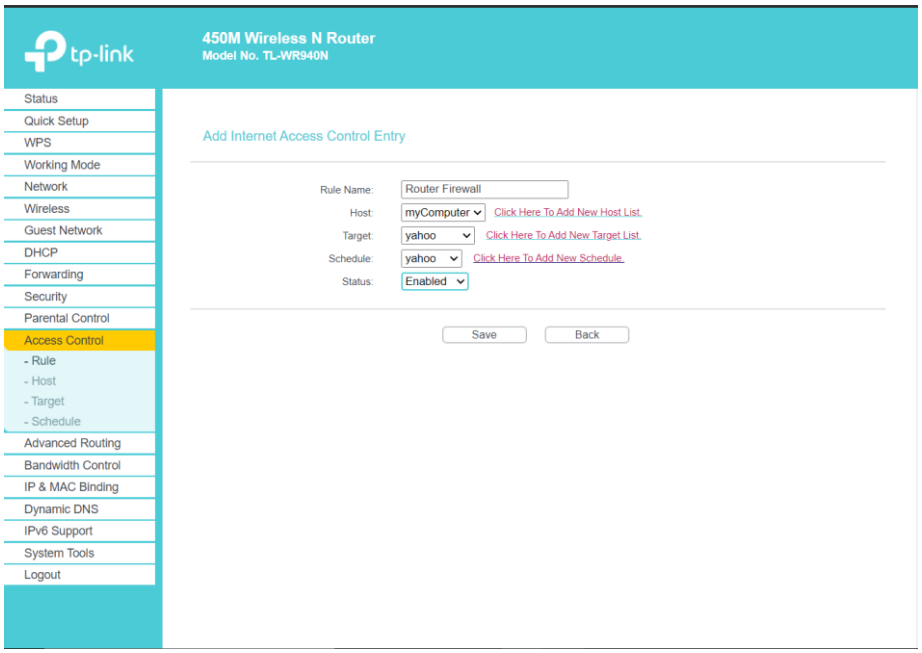


រូបភាពទី ២១ ៖ បង្ហាញពីការកំណត់ Schedule នៅលើ Acess Control

៨.ចូលមកកាន់ Rule ហើយចុចតាមដូចរូបខាងក្រោមដែលបានបង្ហាញ ហើយចុច Save បន្ទាប់មកចូលទៅកាន់ Add New នឹងបំពេញពិត័មានដូចនៅក្នុងរូបដែលបានបង្ហាញនៅផ្នាំងទីពីរ៖

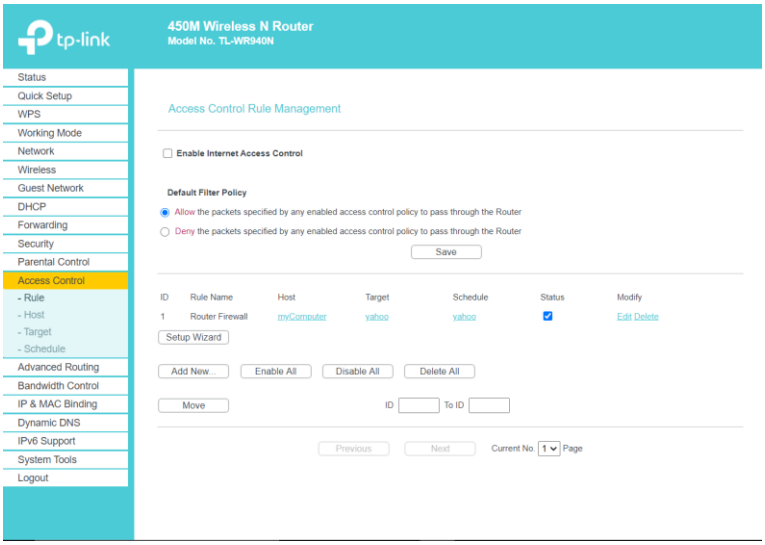


រូបភាពទី ២២ ៖ បង្ហាញពីការកំណត់ Rule នៅលើ Access Control



រូបភាពទី ២៣ ៖ បង្ហាញពីការ Add New Rule នៅលើ Access Control

៩.ចំណុចចុងក្រោយអ្នកនឹងបានឃើញ ទម្រង់បែបនេះដូចក្នុងរូបខាងក្រោម៖



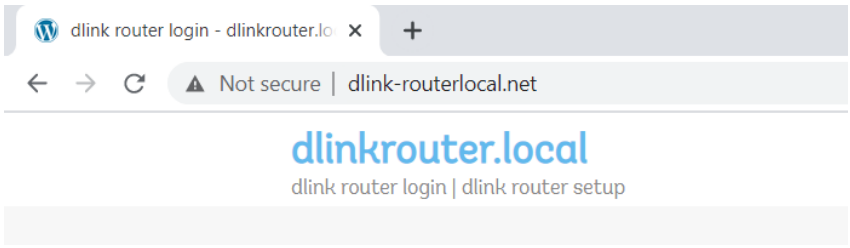
រូបភាពទី ២៤ ៖ បង្ហាញពីដំណាក់កាលចុងក្រោយពេលដំឡើងរួច

ការបើកអោយដំណើរការរបស់ Firewall នៅលើ Wireless Router ត្រូវបានដំណើរការដូចទៅតាមការរៀបរាប់នៅខាងលើ៕

៣.១.២ របៀបនៃការដំឡើង វេប ហ្វៀលធើ (Web Filter)

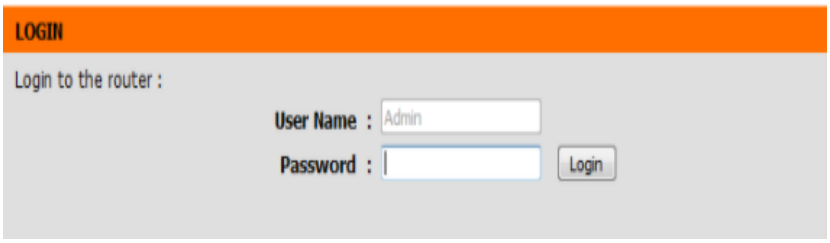
យើងដឹងហើយថា Web Filter មានសារៈសំខាន់ណាស់ក្នុងការចូលរួមជាមួយការតំឡើងនៃណែតវឺក។ ដូចនេះយើងគួរតែដំឡើង Web Filter តាមលំនាំខាងក្រោម៖

១. ដំបូងអ្នកត្រូវបើកវេបប្រោវស្ទើ (Web Browser) នឹងចូលក្នុងប្រភេទរោតទ័ររបស់យើង



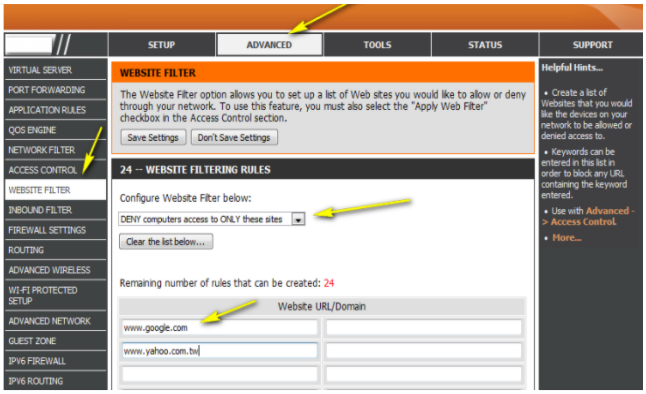
រូបភាពទី ២៥ ៖ បង្ហាញអំពីការចូលក្នុងរោតទ័រតាម Web Browser

២. អ្នកត្រូវតែចូលទៅក្នុង Username នឹង លេខសម្ងាត់របស់អ្នក នៅក្នុង រោតទ័ររបស់អ្នក



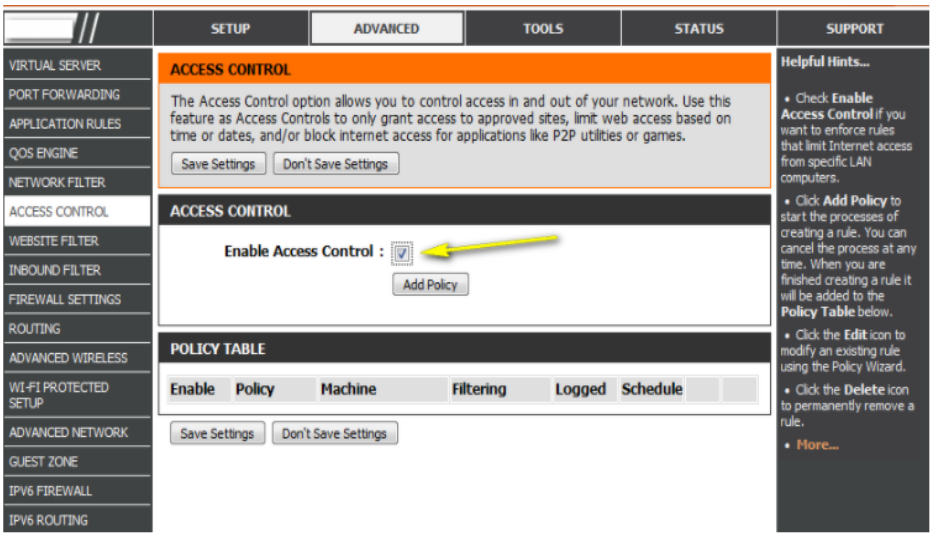
រូបភាពទី ២៦ ៖ បង្ហាញអំពីការវាយឈ្មោះអ្នកប្រើប្រាស់នឹងលេខសម្ងាត់

៣. បន្ទាប់ពីអ្នកចូលទៅក្នុងរោតទ័ររួចហើយ រួចត្រូវស្វែងរក ពាក្យ Advanced Tab បន្ទាប់បកស្វែងរកពាក្យ Website Filter។ ជ្រើសរើសជម្រើស Deny Computer Access to ONLY these site បន្ទាប់វាយ URL ដែលអ្នកចង់បិទមិនអនុញ្ញាត ។បន្ទាប់មកចុចពាក្យ Save Setting ។



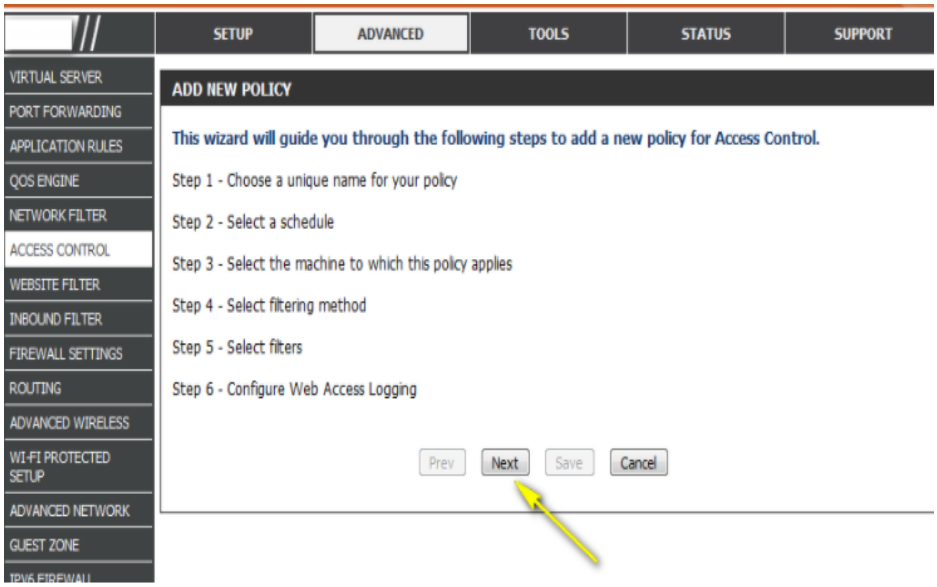
រូបភាពទី ២៧ ៖ បង្ហាញអំពីការជ្រើសរើសនូវប្បាប់ Website Filter

៤. បន្ទាប់អ្នកត្រូវចូលទៅក្នុង Access Control រួចចុចលើ ជ្រើស នៅក្នុង Enable Access Control បន្ទាប់មកចុចលើពាក្យ Add Policy



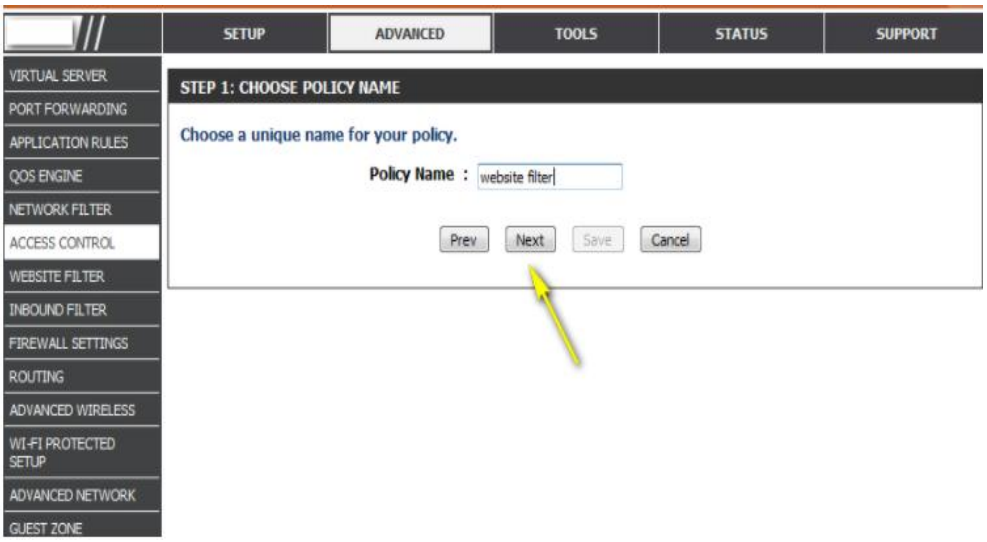
រូបភាពទី ២៨៖ បង្ហាញអំពីការជ្រើសរើសនូវ Access Control

៥. ចុចពាក្យ Next នៅក្នុង Add New Policy



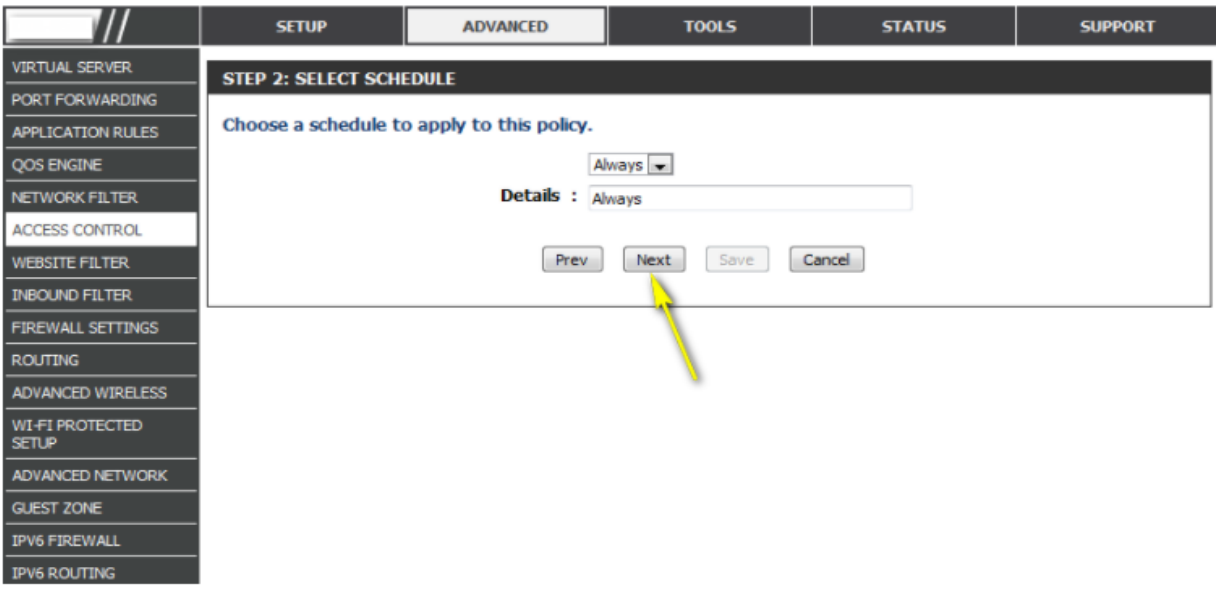
រូបភាពទី ២៩ ៖ បង្ហាញអំពីការចុចពាក្យ Next នៅលើ Add New Policy

៦. បន្ទាប់មកអ្នកត្រូវវាយពាក្យ Website Filter នៅក្នុង Policy Name រួចចុចលើពាក្យ Next



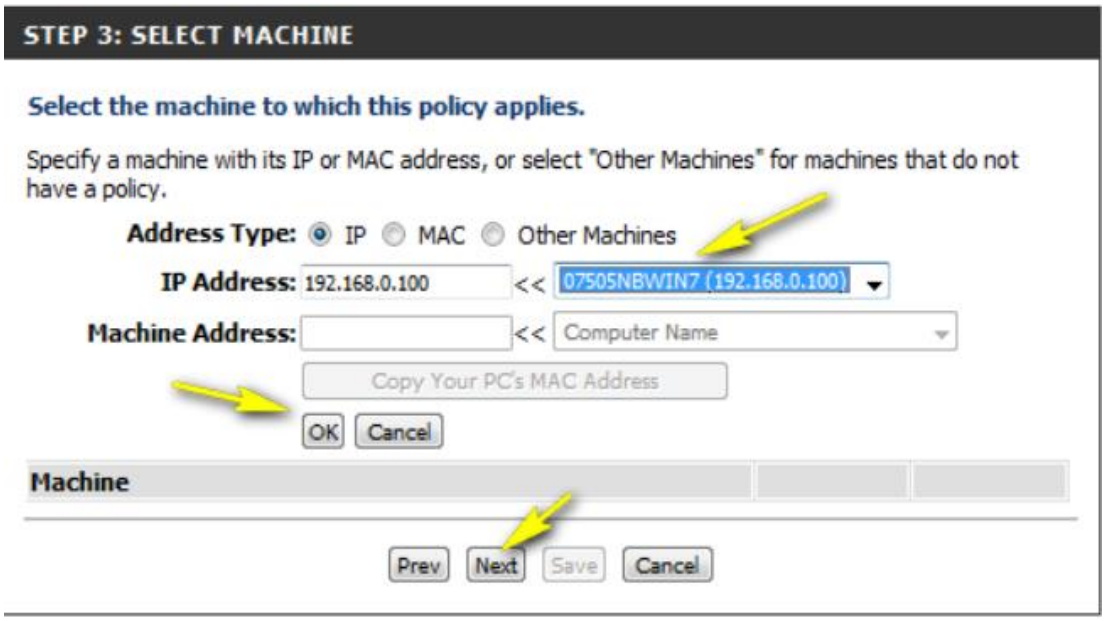
រូបភាពទី ៣០ ៖ បង្ហាញអំពីការវាយពាក្យ Website Filter ក្នុង Policy Name

៧. រួចមកអ្នកត្រូវ Selected Always នឹងវាយពាក្យ Always នៅក្នុង Details រួចចុចពាក្យបន្ទាប់



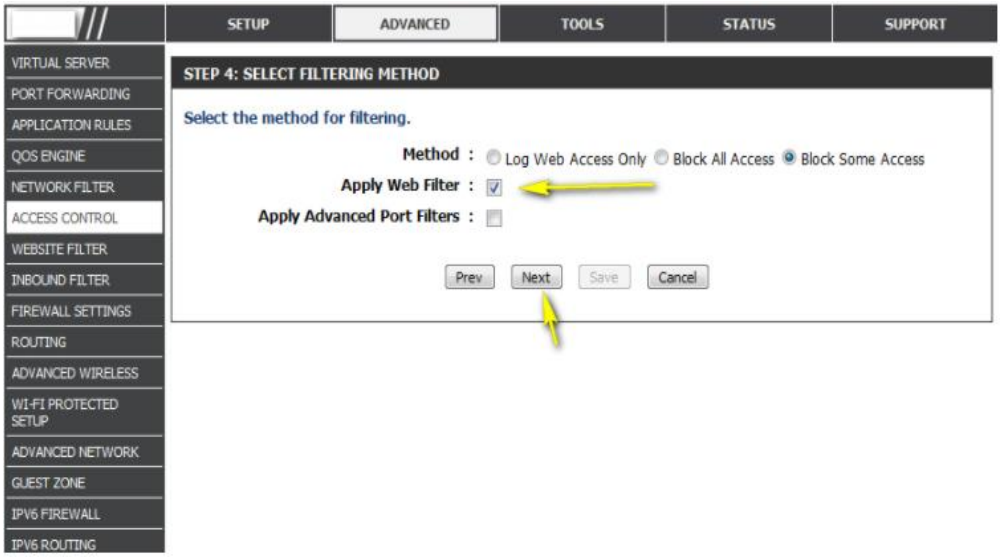
រូបភាពទី ៣១ ៖ បង្ហាញអំពីការវាយពាក្យ Always នឹង ជ្រើសរើស Always

៨. ជ្រើសរើសនូវប្រភេទម៉ាស៊ីនដែលអ្នកចង់ដាក់នៅក្នុង Address Type , IP Address រួចចុចពាក្យ OK បន្ទាប់មកជ្រើសរើសពាក្យ Next



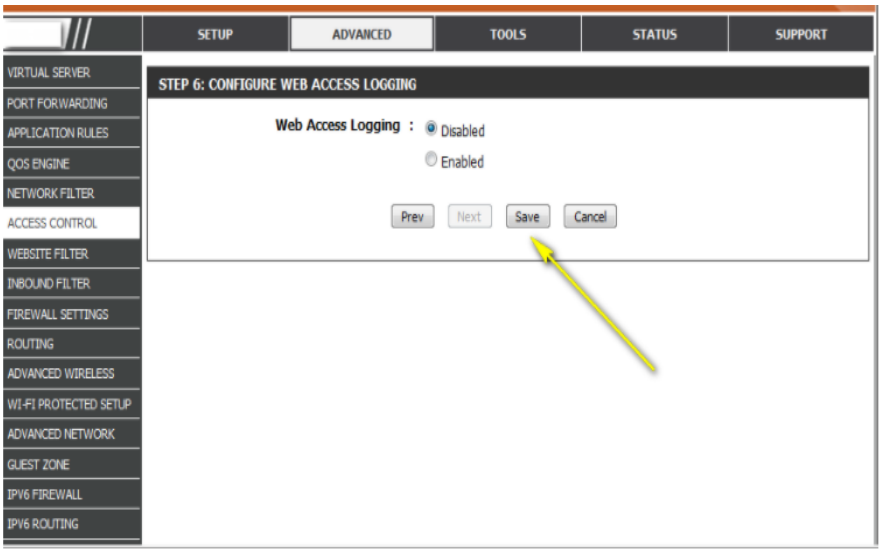
រូបភាពទី ៣២ ៖ បង្ហាញអំពីការរាយ Address Type និង IP Address

៩. ជ្រើសរើសពាក្យ Block Some Access ក្នុង Method ព្រមទាំង ចុច ជ្រើស ក្នុង Apply Web Filter រួចចុចលើពាក្យ Next



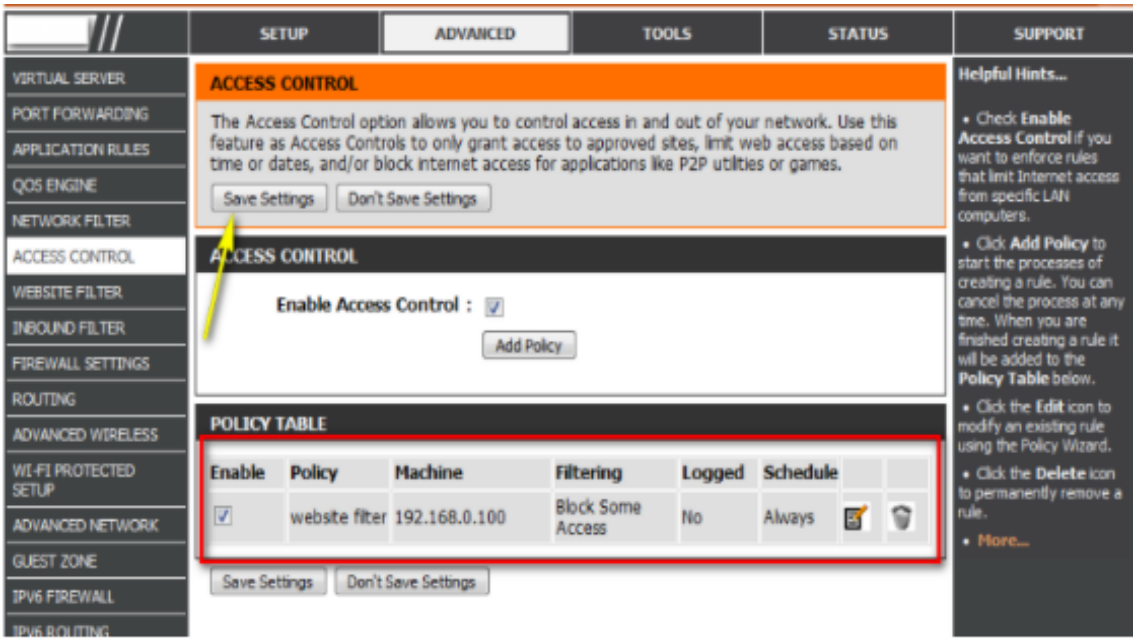
រូបភាពទី ៣៣ ៖ បង្ហាញអំពីការជ្រើសរើសយក Apply Web Filter

១០. បន្ទាប់មកអ្នកត្រូវត្រៀជ្រើសរើសរវាង Disable និង Enable



រូបភាពទី ៣៤ ៖ បង្ហាញអំពីការជ្រើសរើសយក Disable ឬ Enable

១១. រួចអ្នកចុចពាក្យ Save Setting នោះវានឹងលោតឡើងនៅពីក្រោមនៃ Policy Tab ។

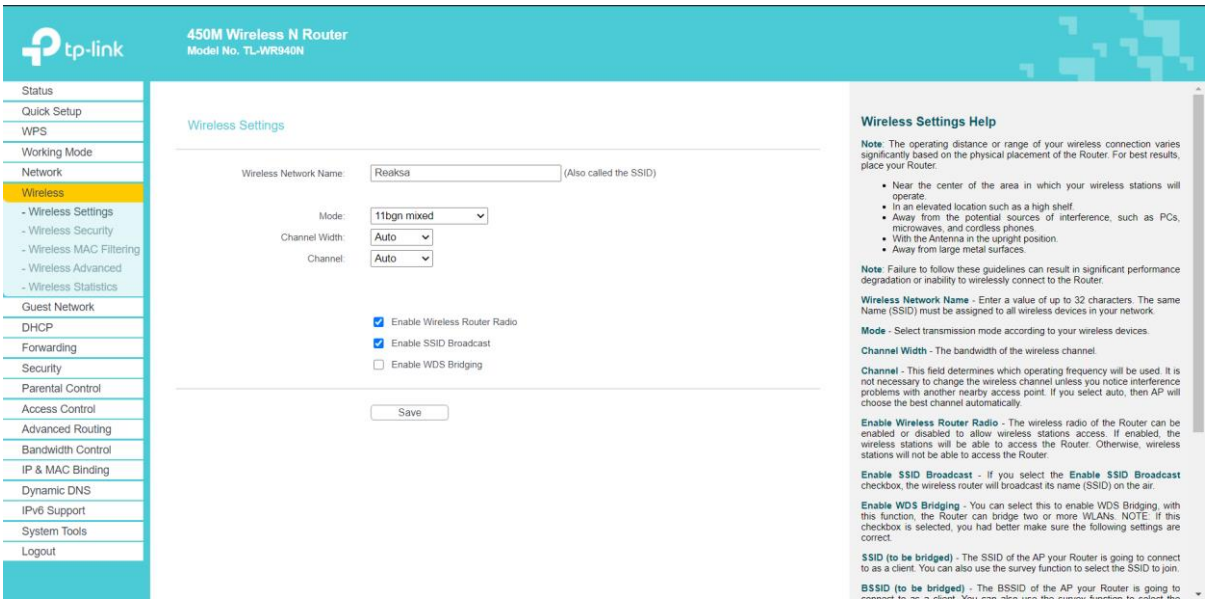


រូបភាពទី ៣៥ ៖ បង្ហាញអំពីការរក្សាទុកនៃ Website Filter

៣.២ សន្តិសុខអាក់សេសភ័ញ្ញ (Access Point Security)

ដើម្បីធ្វើអោយ Wireless Access Point របស់អ្នកមានសុវត្ថិភាពខ្ពស់ យើងសូមណែនាំវិធីសាស្ត្រទាំង ៨ ចំណុចដូចខាងក្រោម៖

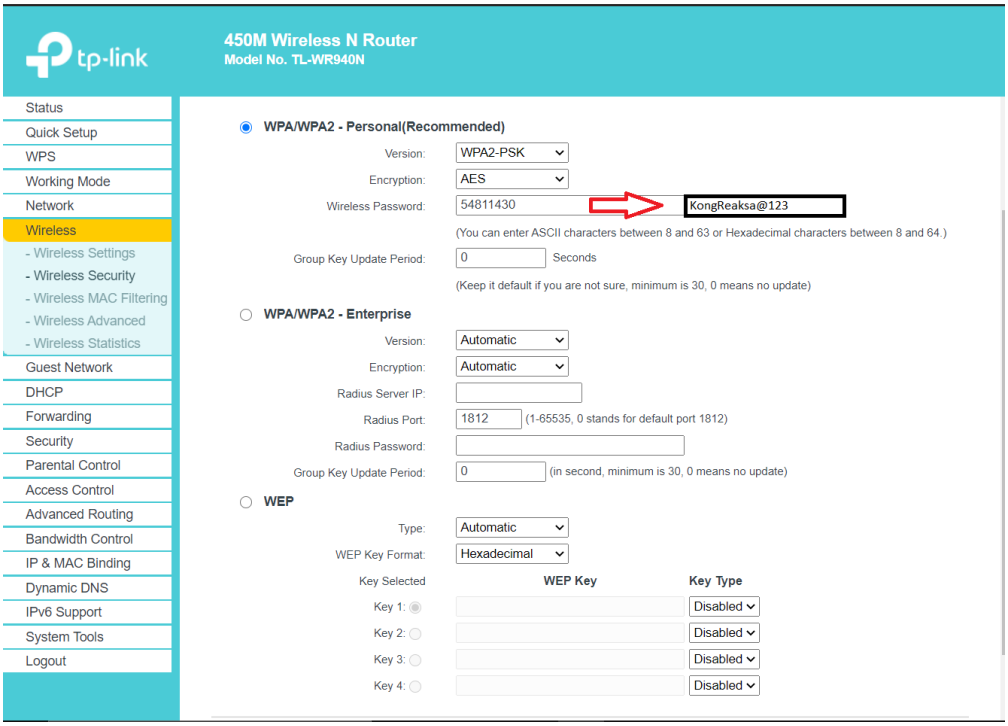
១. នៅខាងក្រោមផ្នែកខាងឆ្វេងនៃពាក្យថា Setup នៃ Window សូមចុចនៅលើពាក្យថា Wireless Setting



រូបភាពទី ៣៦ ៖ បង្ហាញអំពីការបើកដំណើរការ Access Point Security

២. នៅខាងក្រោមពាក្យថា Wireless Network បញ្ចូលឈ្មោះដែលត្រូវបានអោយដឹងថាជា SSID (Service Set Identifier) សម្រាប់ប្រព័ន្ធបណ្តាញរបស់ផ្ទះរបស់អ្នក។ SSID របស់លោកអ្នកអាចមានចំនួនរហូតដល់ទៅ ៣២ តួអក្សរ ដែលជា Case Sensitive (Example: HOME123456789 ដែលវាមានភាពខុសគ្នាពី Home123456789)

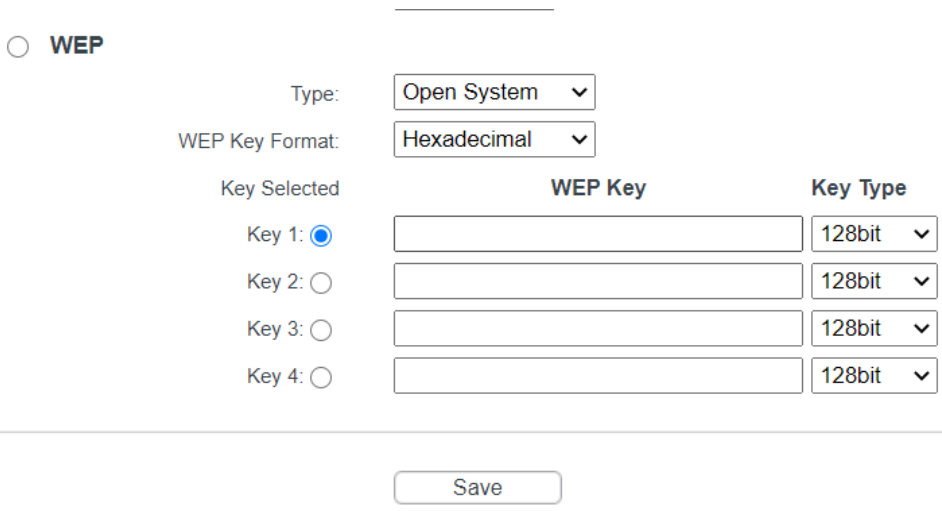
៣. ខាងក្រោម Security Options ជ្រើសរើសយកពាក្យក្នុងចំណោម Setting ដែលមានបង្ហាញដំណើរការបន្ទាប់គឺស្ថិតនៅក្នុងជំហានទី៤ ហើយបន្តបន្ទាប់ទៀតនៅក្នុងជំហានទី៧។ អ្នកគួរតែជ្រើសរើសយកជម្រើសដែលរឹងមាំបំផុតដែលមាននៅក្នុង Wireless Access Point (WPA-PSK [TKIP] + WPA2-PSK [AES]) ហើយប្តូរ Wireless Password។



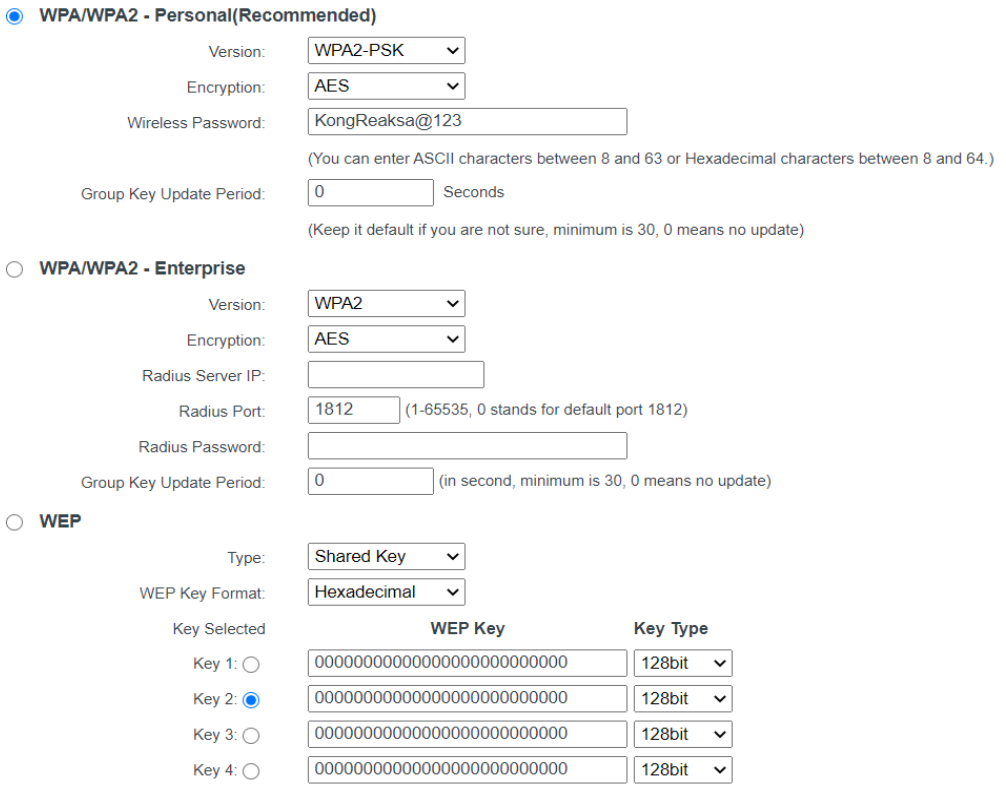
រូបភាពទី ៣៧ ៖បង្ហាញអំពីការប្តូរ នឹង Configure នៅលើ Access Point Security

៤.នៅខាងក្រោមចំណុច Security Encryption(WEP) ប្តូរ Authentication Type ទៅជា Automatic Encryption Strength ទៅជា 64bit or 128 bit. (128 bit គឺជាជម្រើសល្អ) ។ ប្រសិនបើអ្នកមានឧបករណ៍ដែលមិនអាចតភ្ជាប់ទៅកាន់ប្រព័ន្ធបណ្តាញរបស់អ្នកបាន អ្នកគួរតែប្តូរ Authentication Type ទៅជា Open System ឬ Share Key ។ ពេលខ្លះវាមានភាពចាំបាច់សម្រាប់ wireless card ឬ operating systems។

៥.នៅខាងក្រោម Security Encryption (WEP)Key អ្នកអាចបញ្ចូលឃ្លាសម្ងាត់ (passphrase) ហើយចុចលើប៊ូតុង Generate ដើម្បីដំណើរការដោយស្វ័យប្រវត្តិរបស់ WEP keys។ ប្រសិនបើអ្នកជ្រើសរើសយក Encryption Strength 64 bit four keys មានលេខប្រព័ន្ធគោល១៦ ចំនួន១០ខ្ទង់ (0-9 A-F) ត្រូវបានបង្កើតឡើង។ បើអ្នកជ្រើសរើសយក Encryption Strength 128 bit one key មានប្រព័ន្ធគោល១៦ ចំនួន ២៦ខ្ទង់ត្រូវបានបង្កើតឡើង។ ម្យ៉ាងទៀត អ្នកអាចបញ្ចូលប្រព័ន្ធគោល១៦តែមួយ សម្រាប់ WEP ។



រូបភាពទី ៣៨ ៖ បង្ហាញអំពីការ Configure ក្នុង WEP នៅលើ Access Point Security



រូបភាពទី ៣៩ ៖ បង្ហាញអំពីដំណាក់កាលចុងក្រោយ Configure នៅលើ Access Point Security

៦. ចុចពាក្យថា Apply អ្នកបានបញ្ចប់ក្នុងការដំឡើង ប្រសិនបើការដំឡើង WEP មានភាពស្មុគស្មាញពេកអ្នកអាចជ្រើសរើសជម្រើសសុវត្ថិភាពផ្សេងទៀតដូចជា(WPA-PSK [TKIP] + WPA2-PSK [AES]) ដែលវាមានភាពងាយស្រួលក្នុងការដំឡើង នឹងសុវត្ថិភាពខ្ពស់ជាង WEP៕

៧. ប្រសិនបើអ្នកសម្រេចចិត្តជ្រើសរើសយក WPA-PSK [TKIP] ឬ WPA2-PSK [AES] ចុចលើជម្រើសនៅខាងក្រោម Security Options។៕

៨. បញ្ចូលឃ្លាសម្ងាត់(passphrase) ចន្លោះពី ៨ ទៅ ៦៣តួ ហើយបន្ទាប់ចុច Apply។៕

វិធីសាស្ត្រដែលល្អបំផុតរបស់ Wireless Internet Security ប្រសិនបើអ្នកមានជម្រើស ខាងក្រោមនេះគឺជា lists របស់ security protocols ដែលរៀបពីលំដាប់ខ្លាំង ទៅ ខ្សោយ៖

1. WPA3
2. WPA2 Enterprise
3. WPA2 Personal
4. WPA + AES
5. WPA + TKIP
6. WEP
7. Open Network (no security implemented

៣.៣ សន្តិសុខវីនដូ (Endpoint Windows Security)

វីនដូគឺជាប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រពេញនិយមមួយលើពិភពលោក។ មានបច្ចេកទេសជាច្រើនក្នុងការធានាសន្តិសុខលើកុំព្យូទ័រក្នុងបណ្តាញ ជាពិសេស កុំព្យូទ័រដែលភ្ជាប់ទៅអ៊ីនធឺណិត។

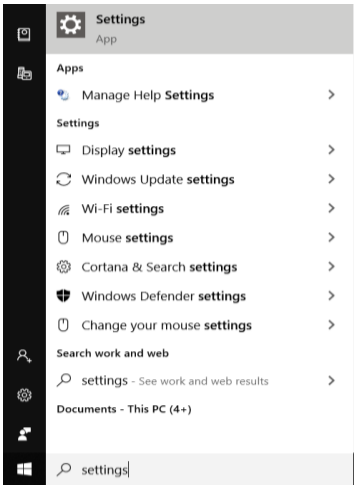
៣.៣.១ អេក្រង់ឆ្លាតរបស់ Windows Defender (Smart Screen)

អេក្រង់ឆ្លាតជួយការពារនិយោជិក ប្រសិនបើពួកគេព្យាយាមចូលមើលគេហទំព័រដែលបានរាយការណ៍ពីមុនថាមានផ្ទុកនូវឧបាយឬម៉ាល់វែរ ហើយដើម្បីបញ្ឈប់ពួកគេពីការទាញយកឯកសារដែលអាចបង្កគ្រោះថ្នាក់។ វាក៏អាចជួយការពារប្រឆាំងនឹងការផ្សាយពាណិជ្ជកម្មក្លែងក្លាយ គេហទំព័របោកប្រាស់ និង រង្វាយប្រហាផ្សេងៗ។

លោក Benoit បានមានប្រសាសន៍ថា "នេះគឺជាផ្នែកមួយនៃស្រទាប់ការពារជាច្រើននៅក្នុងយុទ្ធសាស្ត្រប្រឆាំងឧបាយនិងម៉ាល់វែរ។

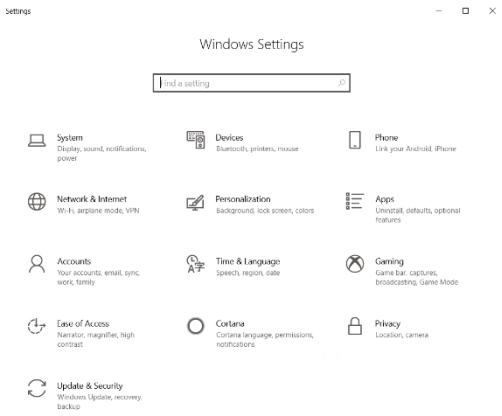
ដើម្បីប្រើប្រាស់នឹងបើកដំណើរការនៃអេក្រង់ឆ្លាតរបស់ Window Defender (Smart Screen) យើងត្រូវធ្វើដូចលំនាំខាងក្រោម៖

១. ចុចប៊ូតុង Start រួចស្វែងរកពាក្យថា Setting



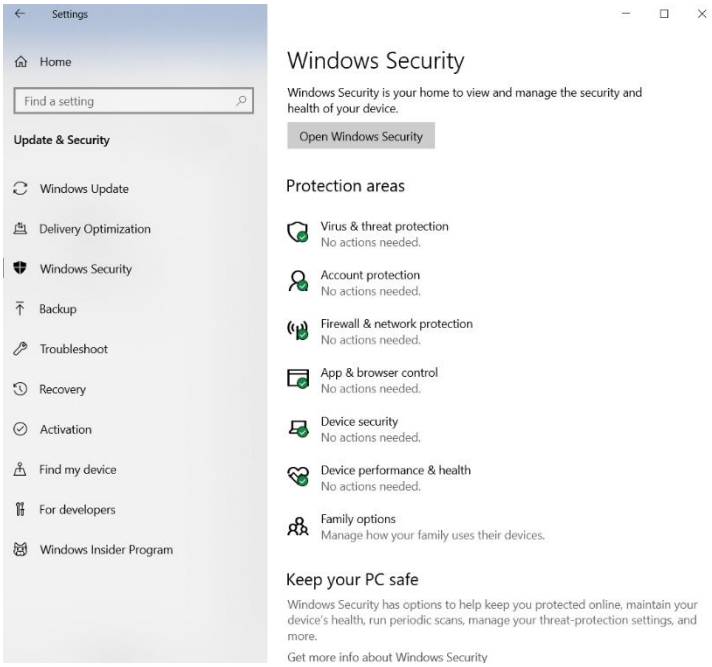
រូបភាពទី ៤០ ៖ បង្ហាញពីផ្ទាំង Search Engine

២. បន្ទាប់មកស្វែងរកពាក្យ Update & Security



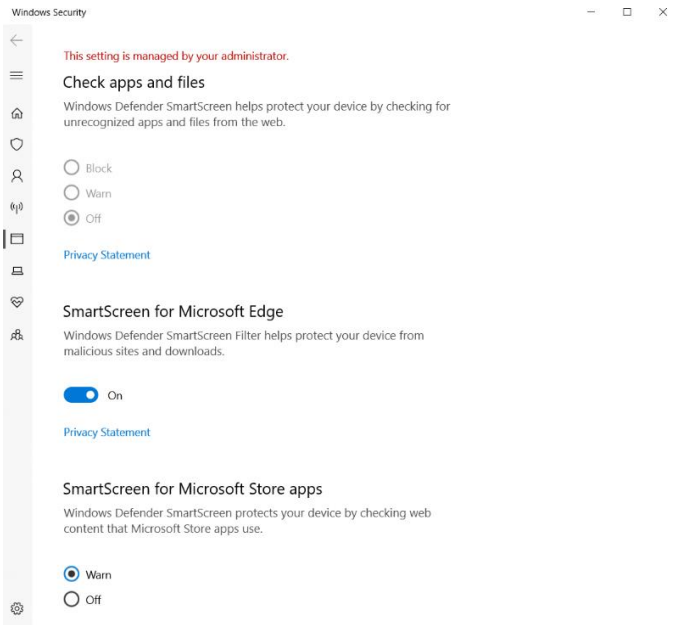
រូបភាពទី ៤១ ៖ បង្ហាញពីផ្ទាំង Setting

៣. បន្ទាប់មកស្វែងរកពាក្យ Update & Security រួចចុចលើ App & Browser Control



រូបភាពទី ៤២ ៖ បង្ហាញផ្ទាំងនៃ Window Security

៤. បន្ទាប់មកបើកដំណើរការនៃ Window Smart Screen



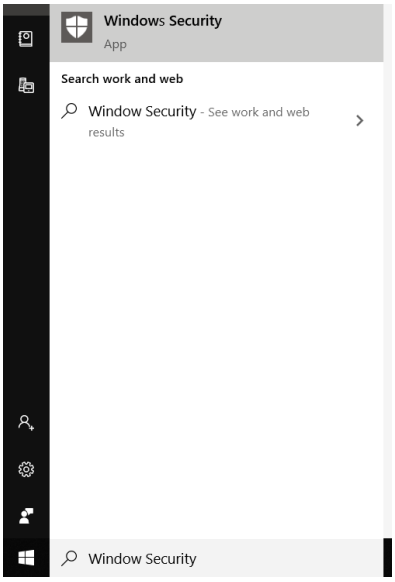
រូបភាពទី ៤៣ ៖ បង្ហាញការបើដំណើរការនៃ SmartScreen

៣.៣.២ កម្មវិធីឆ្មាំរបស់ Windows Defender

កម្មវិធីឆ្មាំផ្តល់ការការពារប្រឆាំងនឹងកិច្ចកំហែងកម្រិតខ្ពស់ ដែលបើករង្វាយប្រហារលើ Microsoft Edge ដោយប្រើបច្ចេកវិទ្យានិម្មិតូបនីយកម្ម Hyper-V របស់ Microsoft ។ មុខងារនេះដំណើរការជាមួយបច្ចេកទេសបញ្ជីស(Whitelist) (អ្នកប្រើអាចកំណត់វេបសាយដែលអាចទុកចិត្ត ដើម្បីអាចច្បាលវាដោយសេរីក្នុងការមើលព័ត៌មាន)។ ប្រសិនបើទំព័រវេបមិនគួរឱ្យទុកចិត្ត កម្មវិធីឆ្មាំនឹងដាក់វាក្នុងកន្លែងមួយ ដោយប្លុកវាទាំងស្រុងពីការចូលប្រើមេម៉ូរី ទីផ្ទុក កម្មវិធី ឧបករណ៍ផ្សេងទៀតលើបណ្តាញ ឬ ធនធានទាំងឡាយដែលជាចំណាប់អារម្មណ៍ចំពោះអ្នករង្វាយប្រហារ។

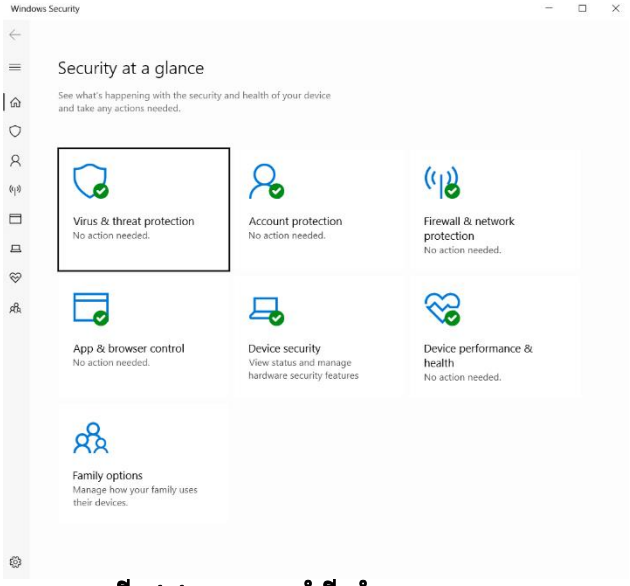
ដើម្បីប្រើប្រាស់នឹងបើកដំណើរការនៃ Window Defender យើងត្រូវធ្វើដូចលំនាំខាងក្រោម៖

១. ដំបូងយើងវាយពាក្យ Window Security នៅក្នុង Search Engine



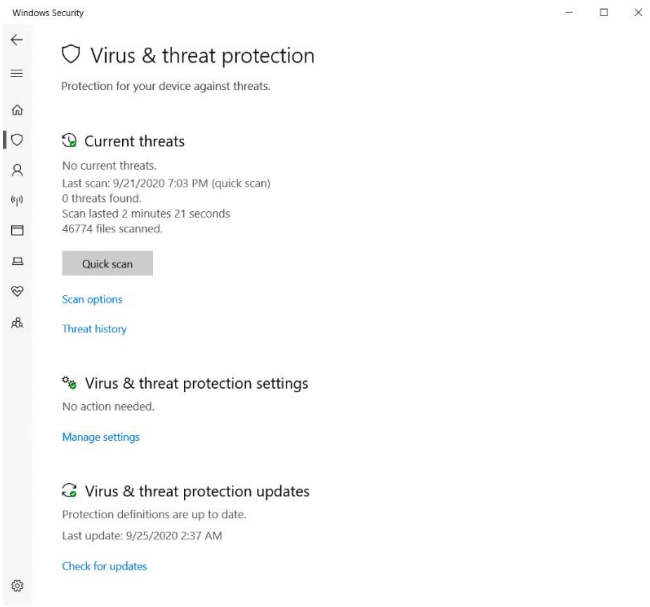
រូបភាពទី ៤៤ ៖ បង្ហាញអំពីផ្ទាំង Search Engine

២. បន្ទាប់មកយើងស្វែងរកពាក្យVirus & Threat Protection រួចលើ វាពីរដង



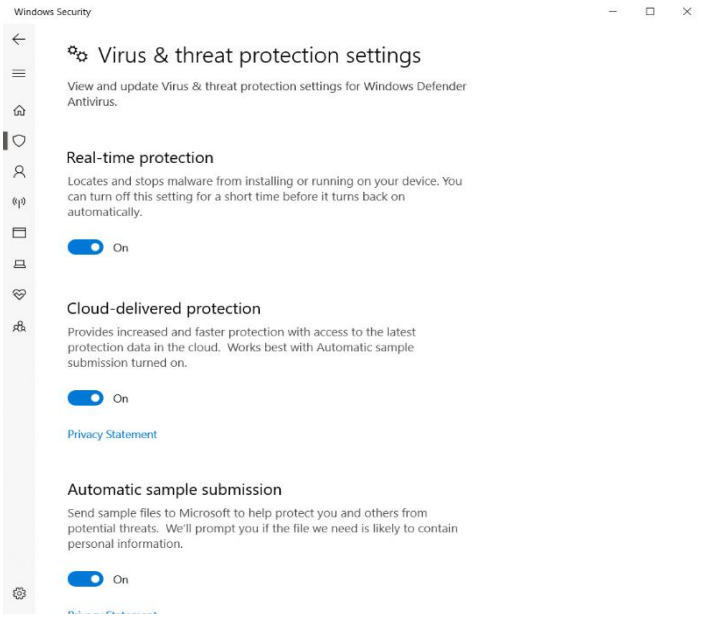
រូបភាពទី ៤៥៖ បង្ហាញអំពីផ្ទាំង Security at a glance

៣. បន្ទាប់មកយើងស្វែងរកពាក្យ Virus & Threat Protection Protection Setting រួចចុចនៅលើ Manage Setting



រូបភាពទី ៤៦ ៖ បង្ហាញអំពីផ្ទាំង Virus & Threat Protection

៤. បន្ទាប់មកយើងស្វែងរកពាក្យ Real-time Protection នឹងបើកដំណើរការ



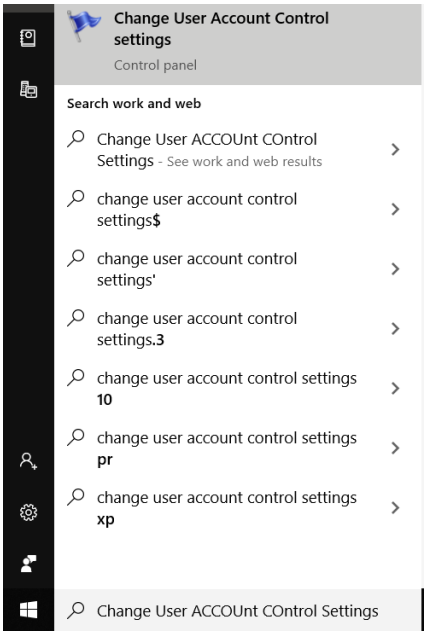
រូបភាពទី ៤៧ ៖ បង្ហាញអំពីការបើកដំណើរការ Window Defender

៣.៣.៣ លក្ខណៈ: User Account Control

UAC ការពារអ្នកប្រើប្រាស់ ដោយរារាំងម៉ាល់វែរពីការបំផ្លាញកុំព្យូទ័រនិងជួយស្តាប័នដាក់ពង្រាយការគ្រប់គ្រង។ ពេលមុខងារនេះបើកដំណើរការ កម្មវិធីនិងភារកិច្ចតែងតែដំណើរការនៅក្នុងបរិបទសន្តិសុខនៃអត្តនាមធម្មតា (non-admin account)។ វាក៏អាចរារាំងដោយស្វ័យប្រវត្តិចំពោះការដំឡើងកម្មវិធីដែលគ្មានការអនុញ្ញាត និងការពារការផ្លាស់ប្តូរដោយចៃដន្យណាមួយចំពោះប្រព័ន្ធ។

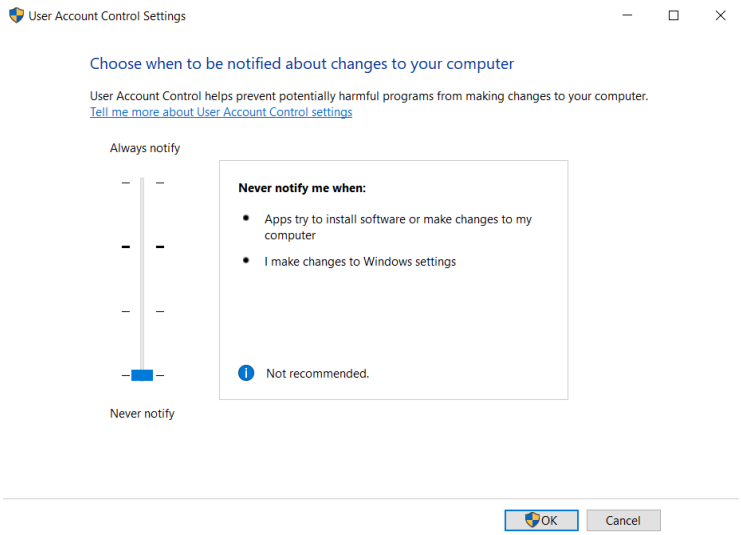
ដើម្បីបើកនូវដំណើរការរបស់ User Account Control យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១. ដំបូងយើងត្រូវចូលក្នុង Search រួចវាយពាក្យថា Change User Account Control Setting



រូបភាពទី ៤៨ ៖ បង្ហាញពីការស្វែងរកនៃ UAC

២. បន្ទាប់មកយើងអាចជ្រើសរើសនូវអ្វីដែលយើងចង់បាន



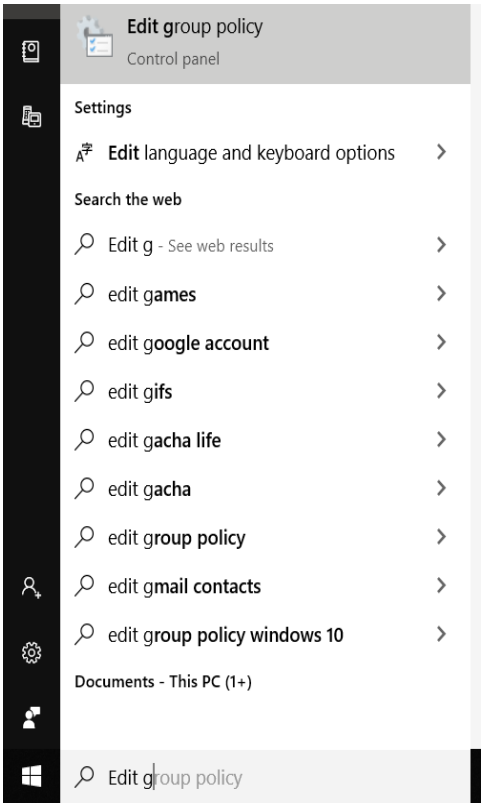
រូបភាពទី ៤៩ ៖ បង្ហាញពីការជ្រើសរើសនៃការប្រើប្រាស់ UAC

៣.៣.៤ ឆ្មាំឧបករណ៍របស់ Windows Defender

លោក Benoit បាននិយាយថា ឆ្មាំឧបករណ៍នេះទាក់ទងនឹងការធ្វើបញ្ជីសលើដ្រាយវើ និងកម្មវិធី។ វាដំណើរការលើសមាសធាតុពីរយ៉ាង៖ ទីមួយ Kernel mode code Integrity (KMCI) ដែលការពារប្រូសេសរបស់ខឺណែលនិងការពារដ្រាយវើ ពីរង្វាយប្រហារថ្ងៃដំបូង (zero-day) និងកម្សាយដទៃទៀតដោយប្រើអេជវីស៊ីអាយ (HVCI)។ ទីពីរ user mode code integrity (UMCI) គឺជាការធ្វើបញ្ជីសកម្មវិធីដែលប្តូកកុំព្យូទ័រ ដោយប្រើត្រឹមតែកម្មវិធីក្នុងបញ្ជី។

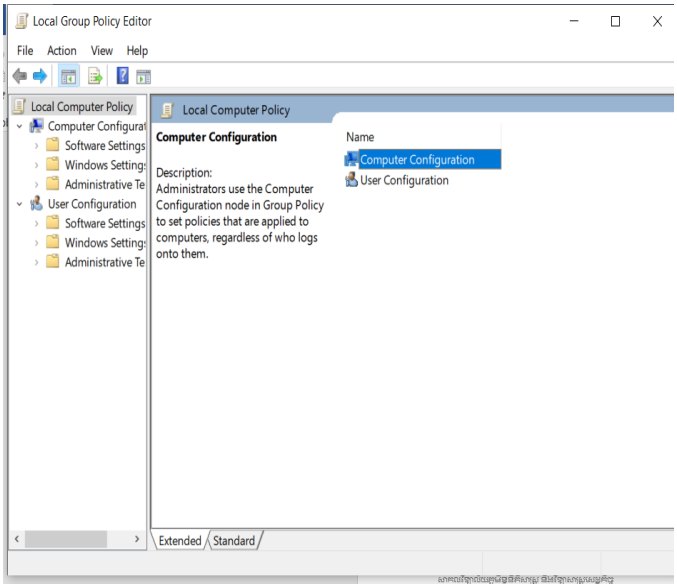
ដើម្បីបើកដំណើរការឆ្មាំឧបករណ៍របស់ Window Defender យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១.ចុចលើ Window Search ស្វែងរកពាក្យ " Edit Group Policy"



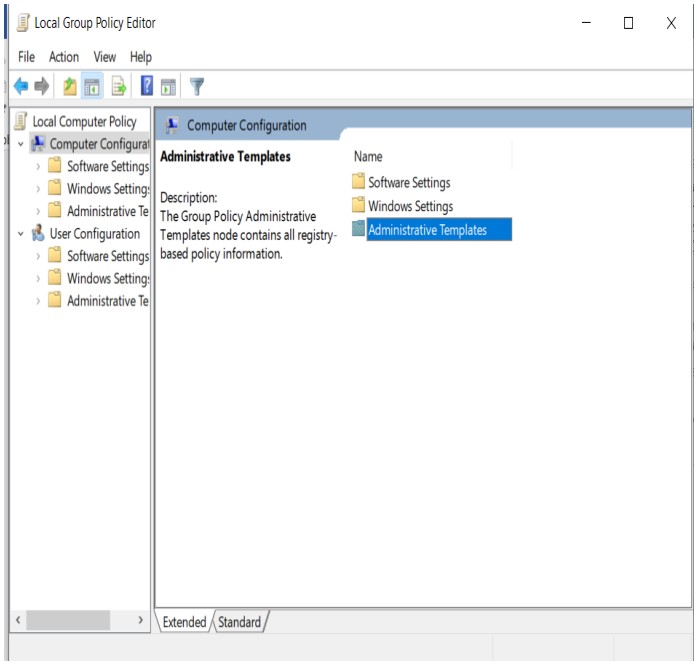
រូបភាពទី ៥០ ៖ បង្ហាញពី Edit Group Policy

២. បន្ទាប់មកចុចលើ Computer configuration



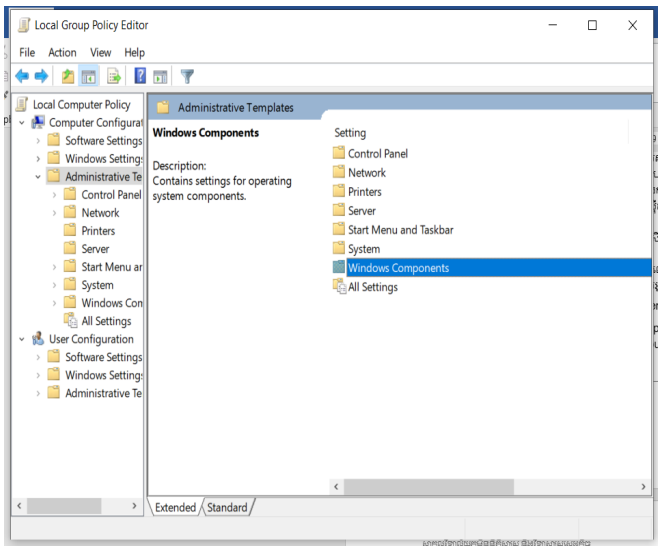
រូបភាពទី ៥១៖ បង្ហាញពី Local Group Policy Editor

៣. រួចចុចលើ Administrative templates.



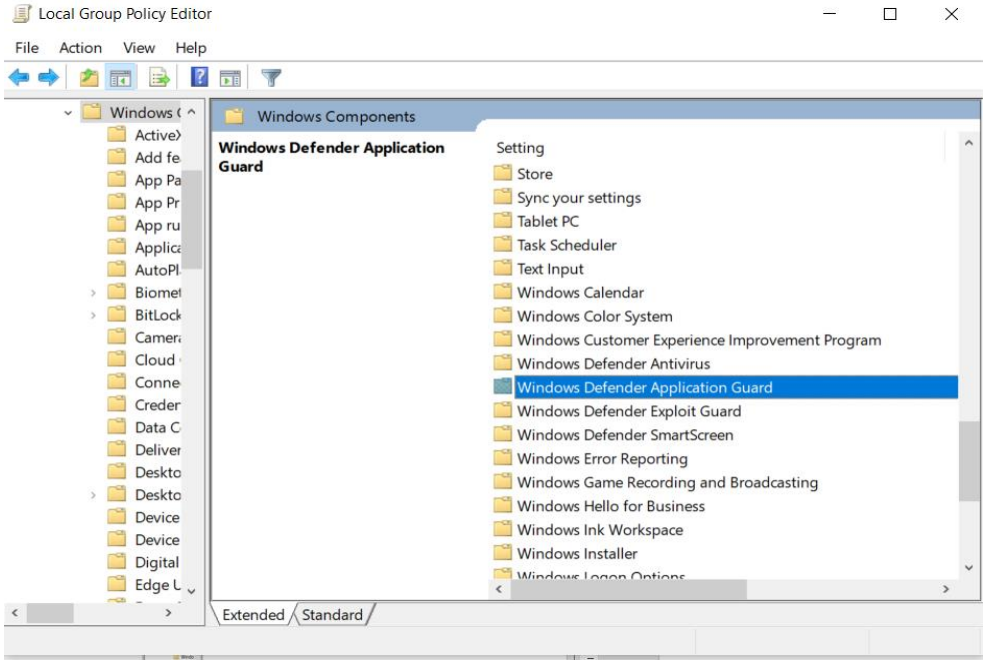
រូបភាពទី ៥២៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

៤. ចុចលើ Windows components



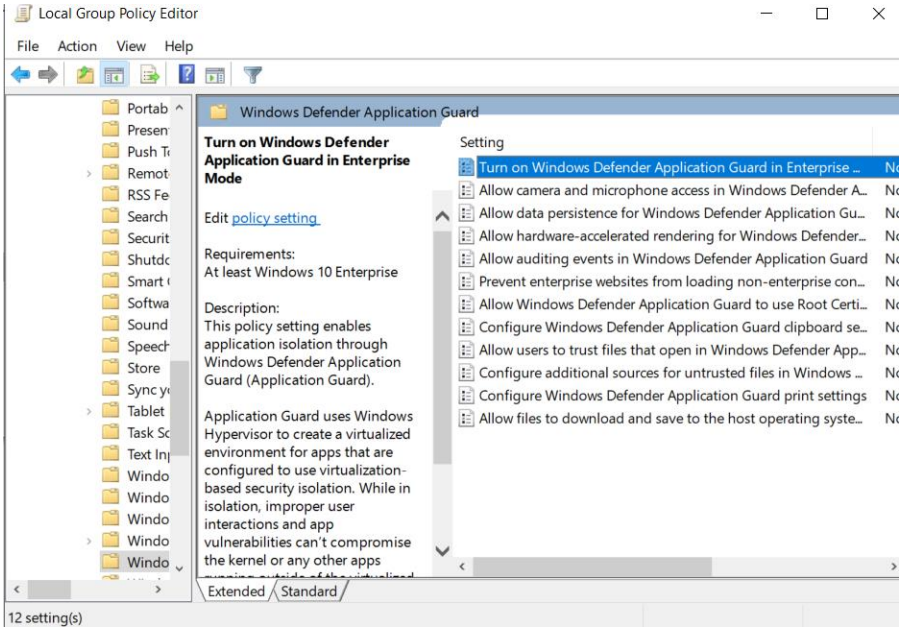
រូបភាពទី ៥៣៖ បង្ហាញពី Window Components

៥. បន្ទាប់មកយើងស្វែងរកពាក្យ Window Defender Application Guard



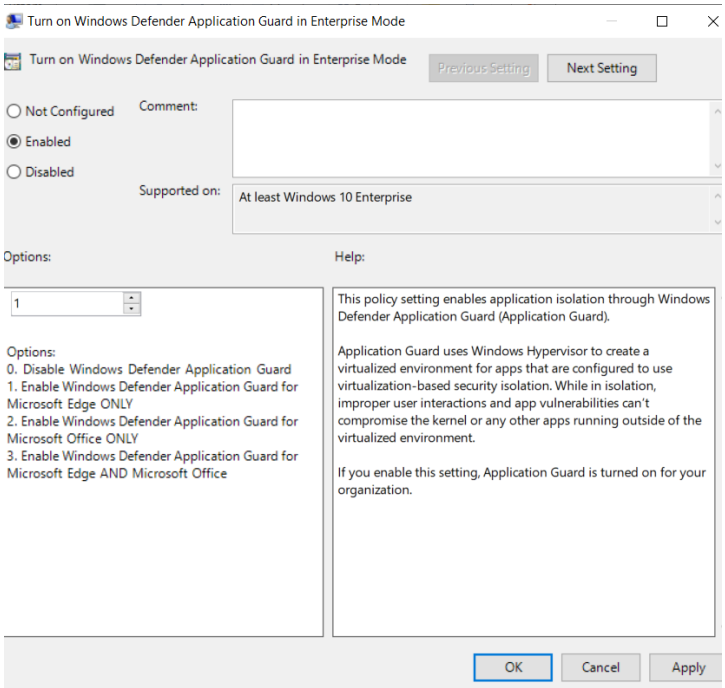
រូបភាពទី៥៤ ៖ បង្ហាញពីផ្ទាំង Window Defender Application Guard

៦. បន្ទាប់មកយើងចុចលើពាក្យ Turn on Window Application Guard



រូបភាពទី ៥៥ ៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard

៧. បន្ទាប់មកយកពាក្យថា Enable រួច Apply បន្ទាប់មកចុចពាក្យ OK



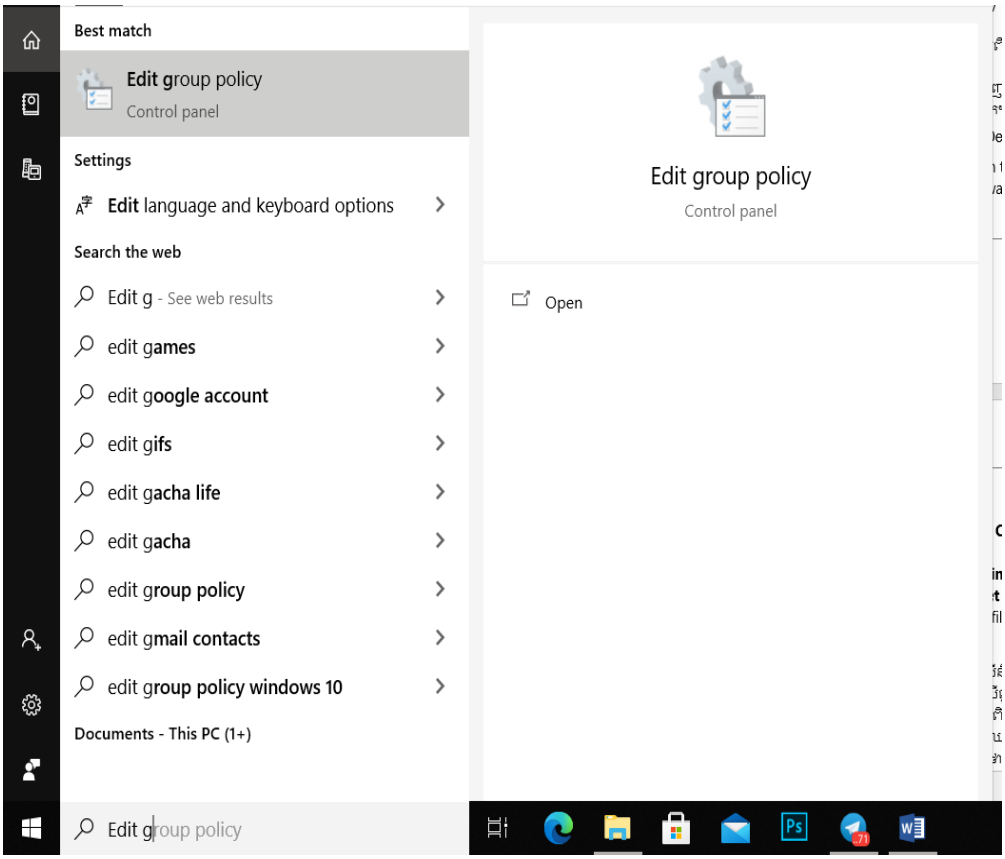
រូបភាពទី ៥៦ ៖ បង្ហាញពីផ្ទាំងពីការបើកនៃ Window Application Guard

៣.៣.៥ ឆ្មាំ Exploit របស់ Windows Defender

ឆ្មាំ Exploit ជាប្រព័ន្ធបង្ការល្បួចរបស់វីនដូ ដែលអាចការពារប្រឆាំងនឹងរង្វាយប្រហារផ្សេងៗ និងការពារកម្សោយនៅក្នុងវីនដូ។ វាក៏អាចការការពារកម្មវិធីចាស់ៗផងដែរ រួមមានឆ្មាំកូដ ប្តូករូបភាព ប្តូកពុម្ពអក្សរមិនស្គាល់។ លោក Benoit បានប្រសាសន៍ថា លក្ខណៈនេះជួយសវនាការ កំណត់រចនាសម្ព័ន្ធនិងគ្រប់គ្រងការបន្ទូបន្តយ Exploit ប្រព័ន្ធនិងកម្មវិធីរបស់វីនដូ ហើយវាក៏ផ្តល់ប្រភេទសមត្ថភាពថ្មីសម្រាប់រារាំងល្បួច" ។

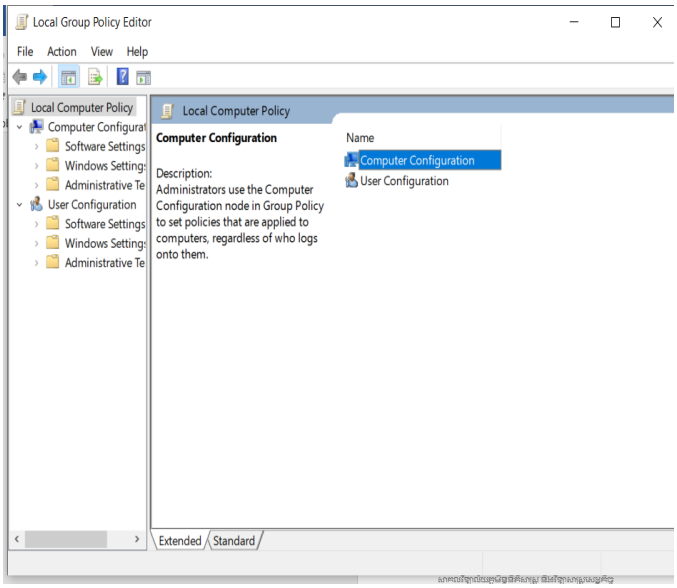
ដើម្បីបើកដំណើរការឆ្មាំ Explorit របស់ Window Defender យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១.ចុចលើ Window Search ស្វែងរកពាក្យ “ Edit Group Policy”



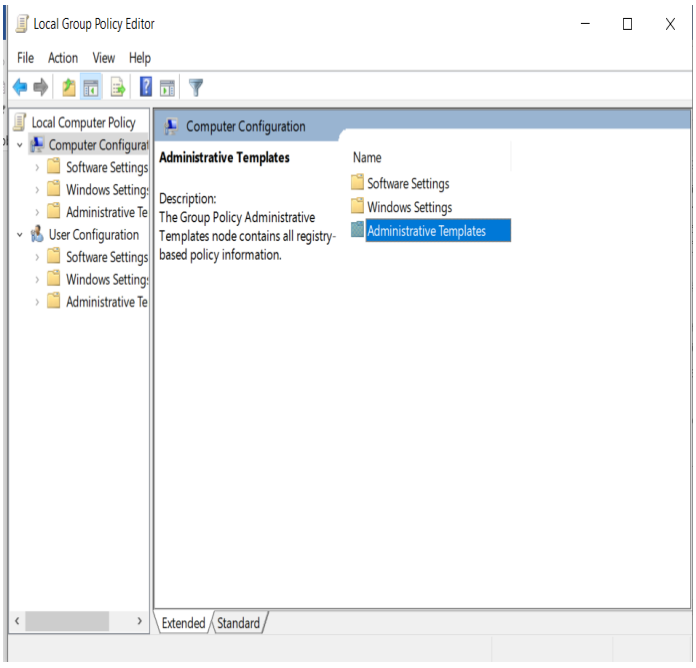
រូបភាពទី ៥៧ ៖ បង្ហាញពី Edit Group Policy

២. បន្ទាប់មកចុចលើ Computer configuration



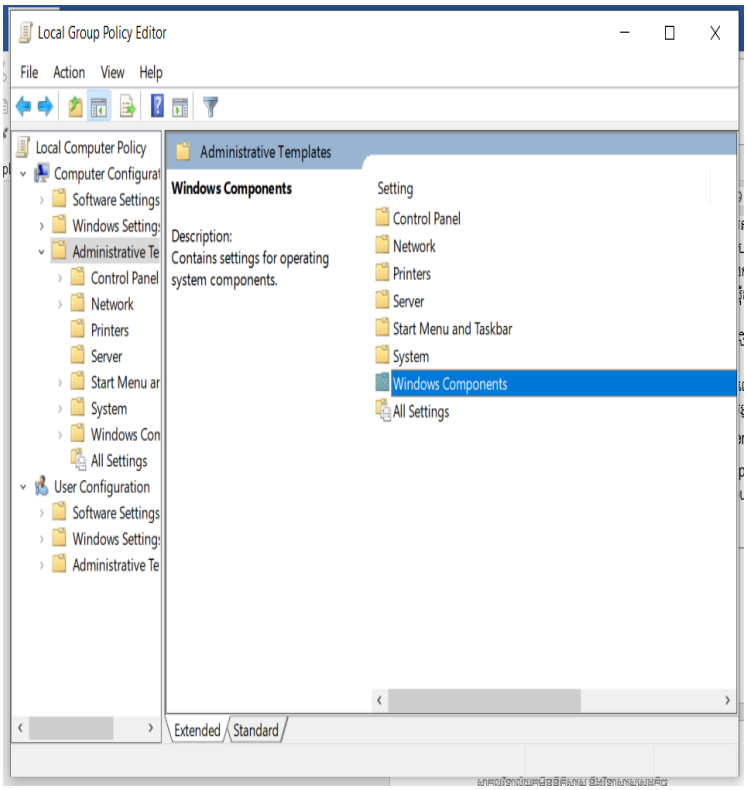
រូបភាពទី ៥៨៖ បង្ហាញពី Local Group Policy Editor

៣. រួចចុចលើ Administrative templates.



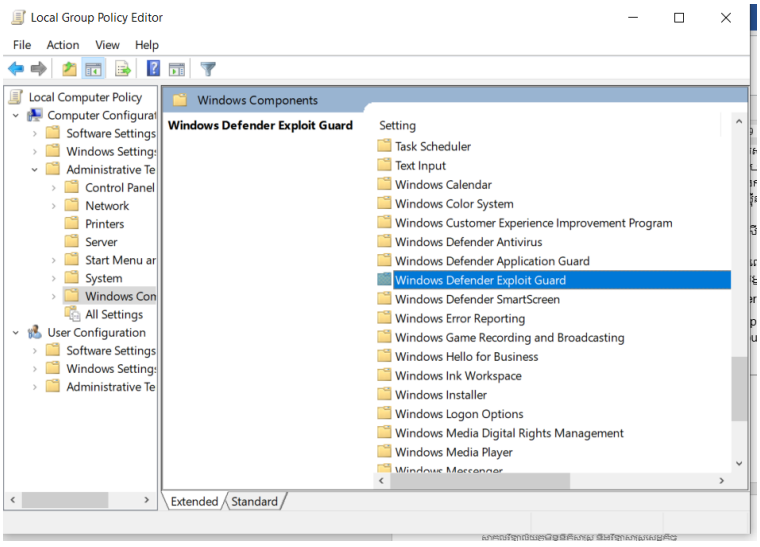
រូបភាពទី ៥៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

៤. ចុចលើ Windows components



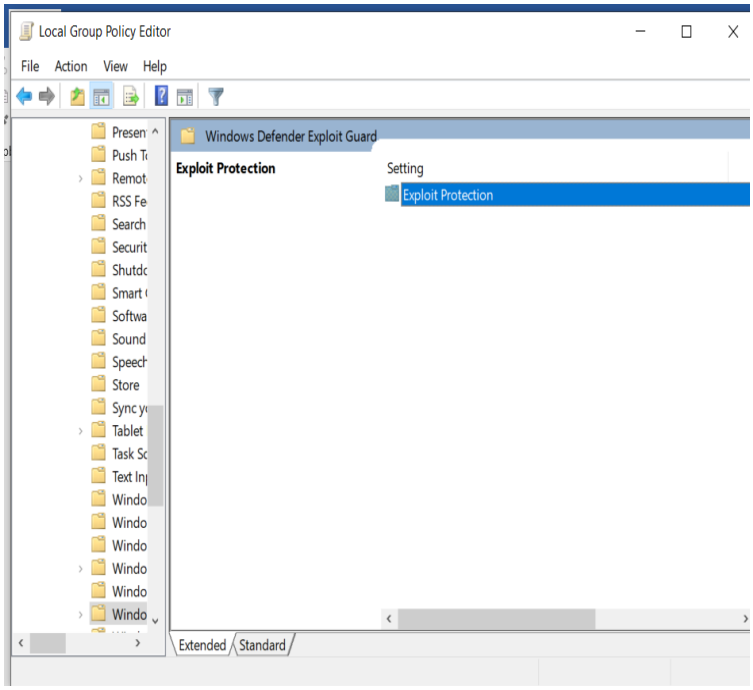
រូបភាពទី ៦០៖ បង្ហាញពី Window Components

៥. បន្ទាប់មកចុចលើ Windows Defender Exploit Guard



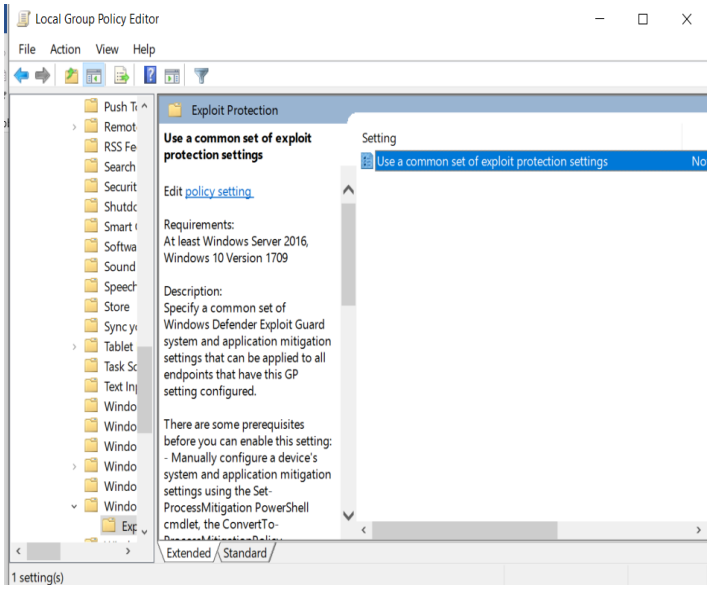
រូបភាពទី ៦១៖ បង្ហាញពី Window Defender Exploit Guard

៦.បន្ទាប់មកចុចលើExploit Protection



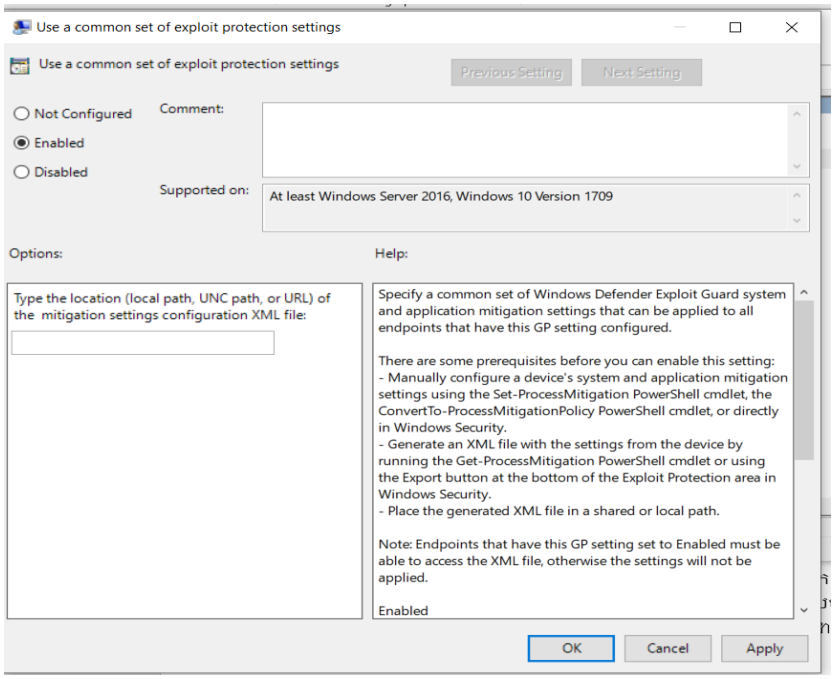
រូបភាពទី ៦២៖ បង្ហាញពី Exploit

៧.បន្ទាប់មក ចុចលើ Use a common set of exploit protection settings.



រូបភាពទី ៦៣ ៖ បង្ហាញពី Use a common set of exploit protection

៨.ចុចលើ **Enabled** and រួចចុចពាក្យ **OK**.



រូបភាពទី ៦៥៖ បង្ហាញពី Enable Window Defender Exploit Guard

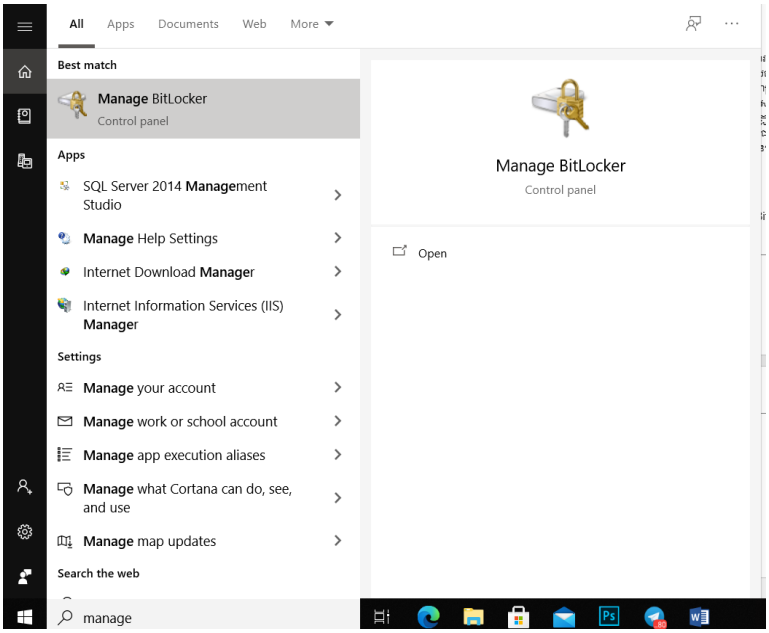
៣.៣.៦ Microsoft Bitlocker

លោក Benoit បានមានប្រសាសន៍ថា "Bitlocker គឺជាដំណោះស្រាយកូដនីយកម្មទូទាំងដ្រាយក្នុងវីនដូ ១០ Professional និង Enteprise។ វាជួយកាត់បន្ថយអាក់សសទិន្នន័យដែលគ្មានការអនុញ្ញាត ដោយពង្រឹងការការពារប្រព័ន្ធនិងឯកសារ និងបញ្ជូនទិន្នន័យដែលមិនអាចអាក់សេសបាន ប្រសិនបើកុំព្យូទ័រត្រូវបានបំបែកឬកែច្នៃឡើងវិញ។

លោកបានបន្ថែមថា "នេះពិតជាសំខាន់ណាស់ - អ្នកមិនចង់ក្លាយជាមនុស្សដែលត្រូវបានស្តីបន្ទោស បន្ទាប់ពីបាត់បង់ឧបករណ៍ ទិន្នន័យ លេចធ្លាយព័ត៌មានរបស់ស្ថាប័ន " ។

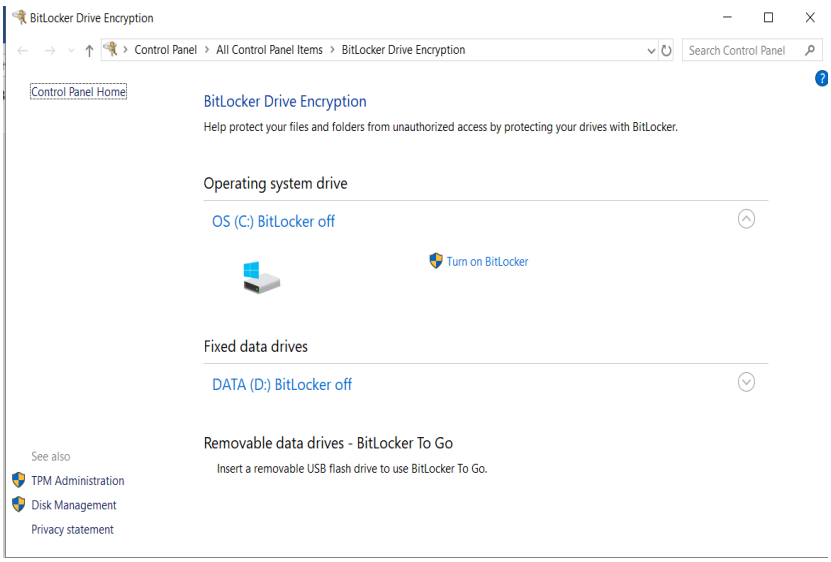
ដើម្បីបើកដំណើរការនៃ Microsoft Bitlocker យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១. ចុចលើ Window Search ហើយស្វែងរកពាក្យ Manage BitLocker



រូបភាពទី ៦៥៖ បង្ហាញពី Manage BitLocker

២. Turn on BitLocker



1

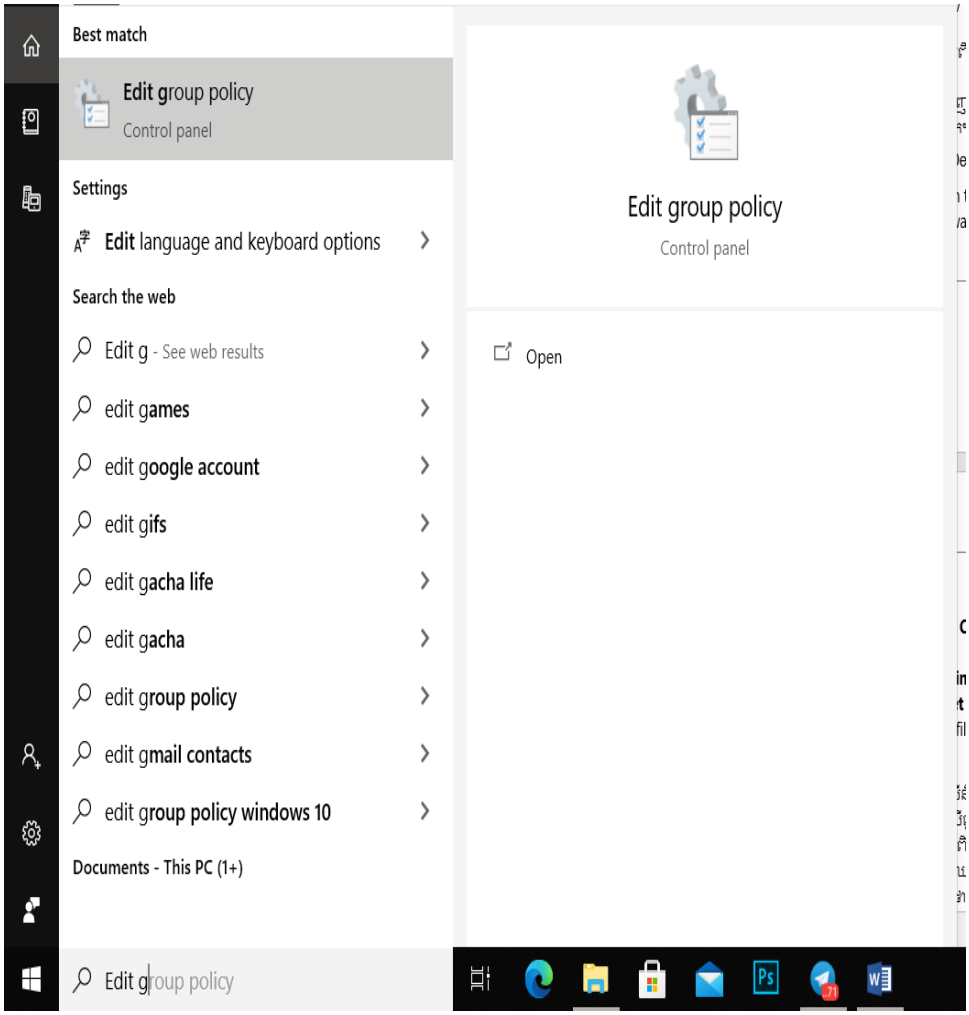
រូបភាពទី ៦៦ ៖ បង្ហាញពី Turn On BitLocker

៣.៣.៧ ឆ្មាំ Credential **របស់** Windows Defender

ឆ្មាំ Credential ជាបច្ចេកទេសសន្តិសុខនិម្មិតក្នុងការដាក់ទិន្នន័យសម្ងាត់ឱ្យនៅដាច់ដោយឡែក ដើម្បីឱ្យត្រឹមតែប្រព័ន្ធប្រតិបត្តិការប៉ុណ្ណោះអាចធ្វើការអាក់សេសវា ដោយការពារពីវង្វាយប្រហារលួចអត្តនាម (user account)។ លក្ខណៈនេះផ្តល់នូវសន្តិសុខហាដវែរនិងការការពារប្រសើរជាងមុនប្រឆាំងនឹងកិច្ចកំហែងឥតឈប់ឈរ។

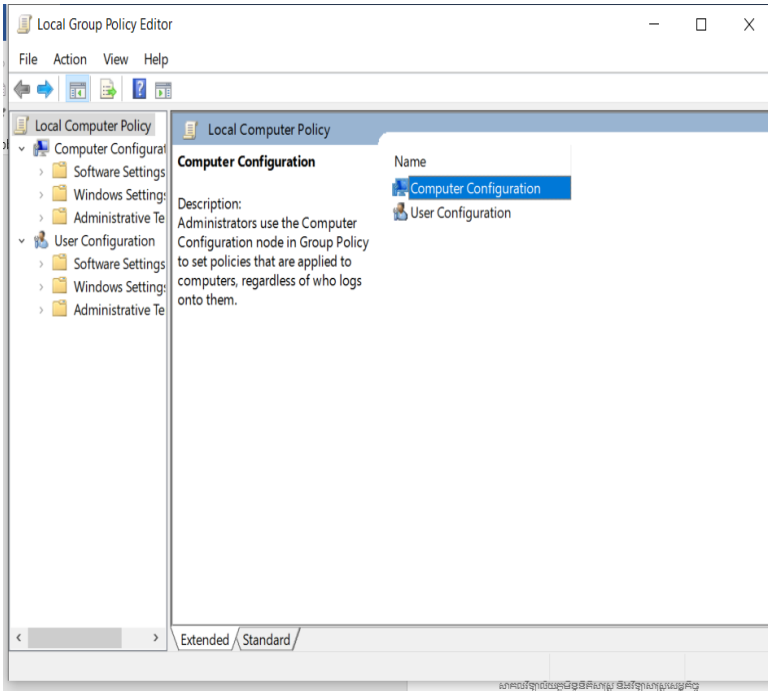
ដើម្បីបើកដំណើរការឆ្មាំ Credential របស់ Window Defender យើងត្រូវធ្វើតាមលំនាំដូចខាងក្រោម៖

១. ចុចលើ Window Search រួចវាយ ពាក្យ Edit Policy Group



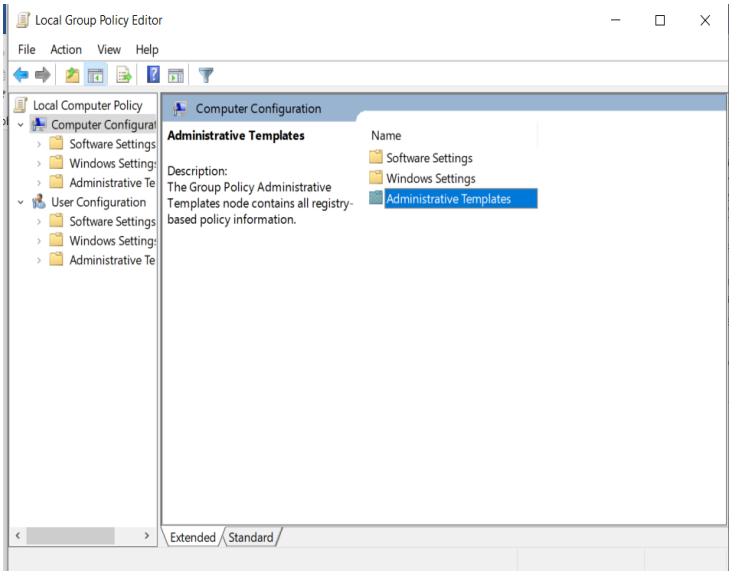
រូបភាពទី ៦៧ ៖ បង្ហាញពី Edit Group Policy

២. បន្ទាប់មកចុចយកពាក្យ Computer Configuration



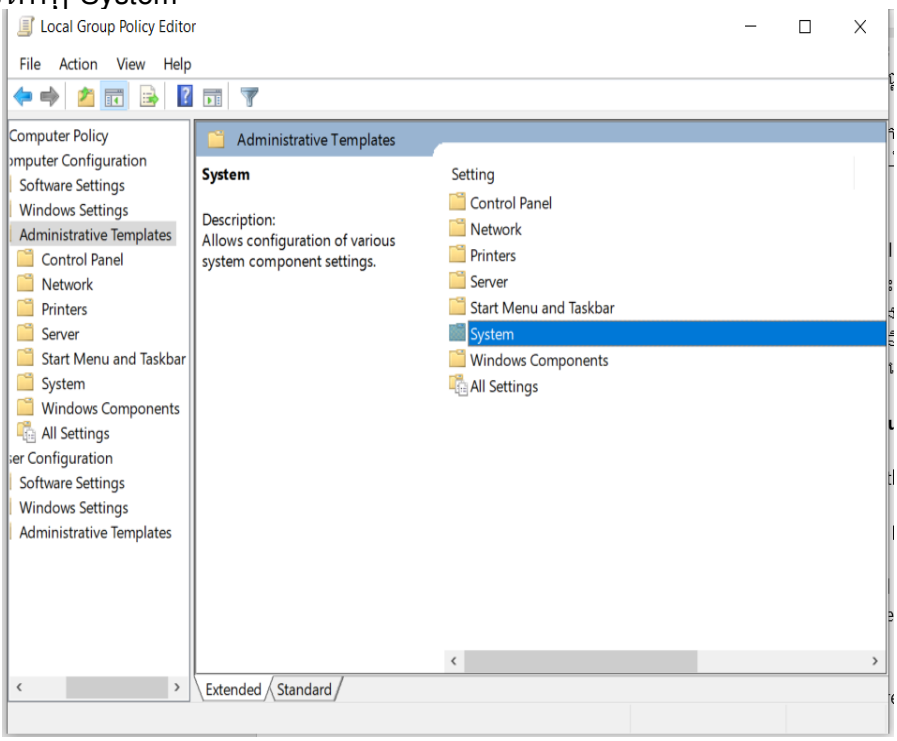
រូបភាពទី ៦៨៖ បង្ហាញពី Local Group Policy Editor

៣. បន្ទាប់មកចុច លើ Administrative Templates



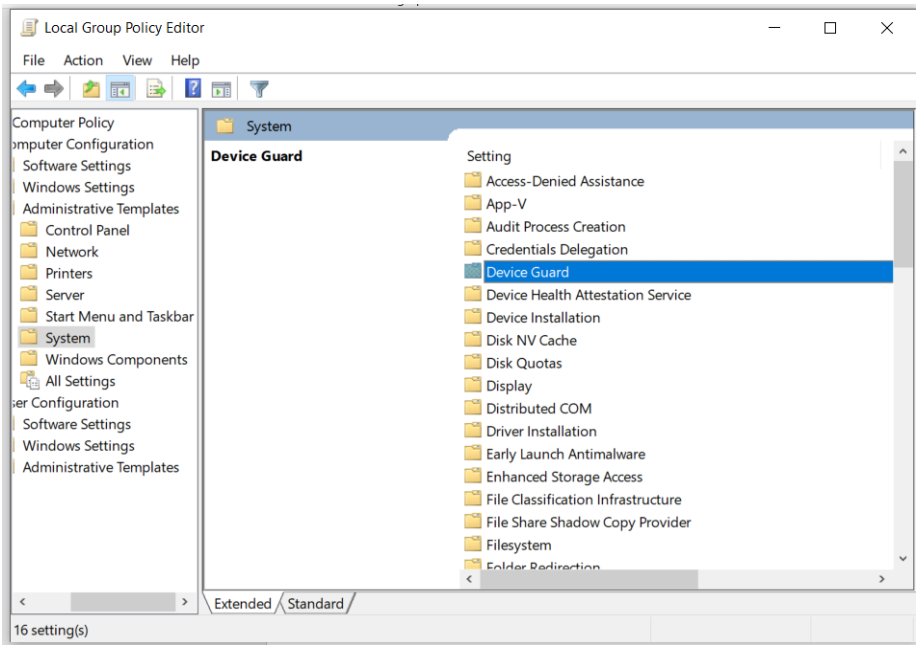
រូបភាពទី ៦៩៖ បង្ហាញពី Administrative ក្នុង Local Group Policy Editor

៤. រួចចុចលើពាក្យ System



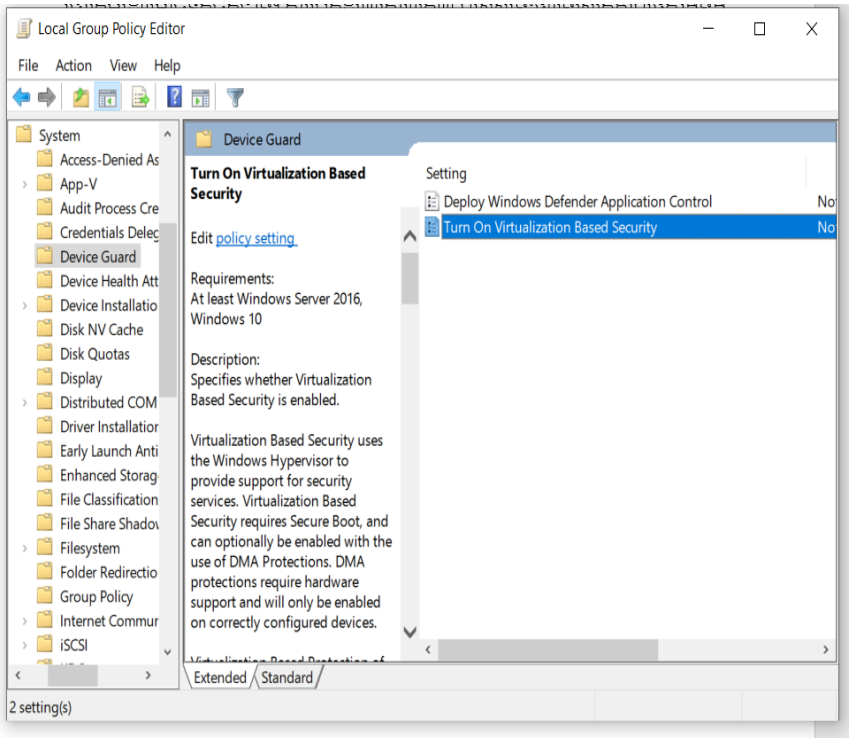
រូបភាពទី ៧០៖ បង្ហាញពី System នៅក្នុង Local

៥. បន្ទាប់មកចុច Device Guard



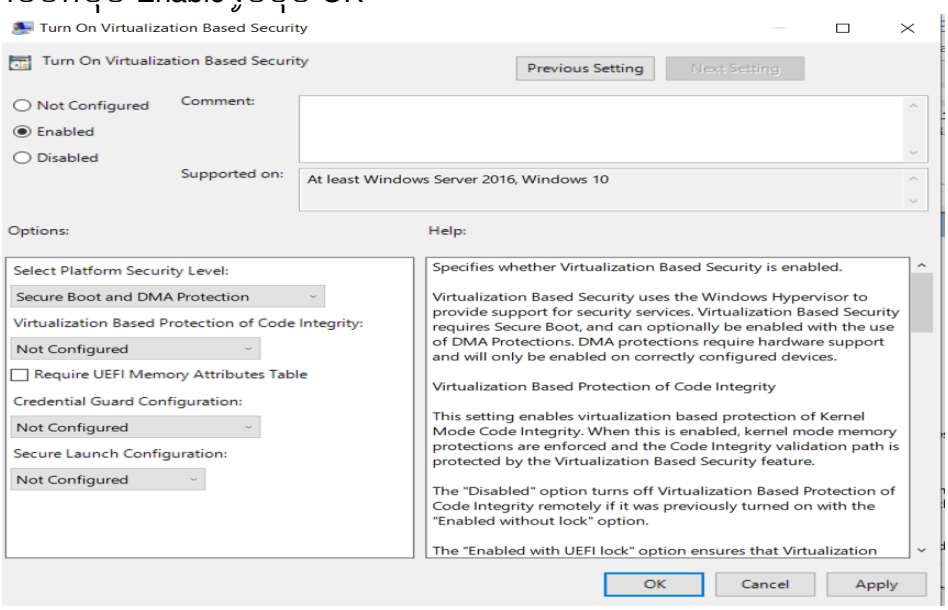
រូបភាពទី ៧១៖ បង្ហាញពី Device Guard នៅក្នុង Local Group Policy

៦. ចុចលើពាក្យ Turn on Virtualization Based Security



រូបភាពទី ៧២៖ បង្ហាញពី Turn on Virtualization Based Security

៧. បន្ទាប់មកចុច Enable រួចចុច OK



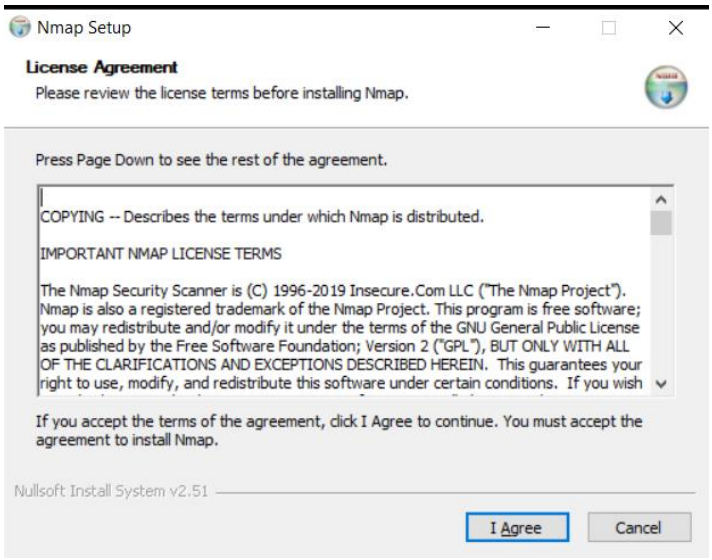
រូបភាពទី ៧៣៖ បង្ហាញពី Enable Window Defender Credential Guard

៣.៤ តេស្តសន្តិសុខ (Security Testing)

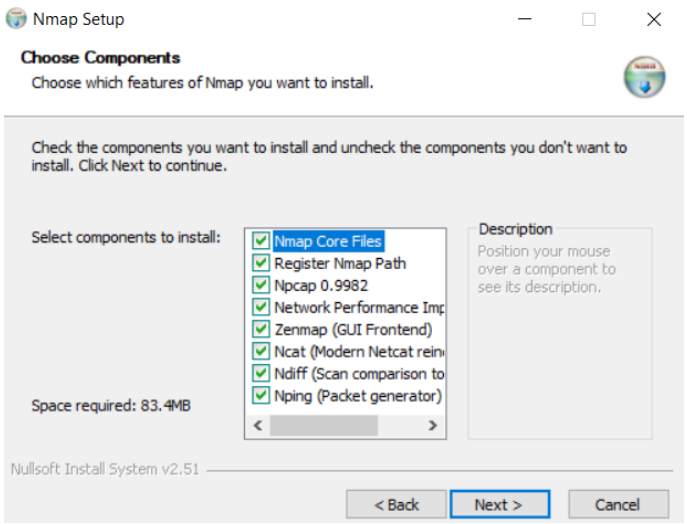
៣.៤.១ របៀបតំឡើងនៃសូហ្វ៊ែ Nmap

ដើម្បីតំឡើងកម្មវិធី យើងគួរតែធ្វើតាមលំនាំនៃការតំឡើងដូចខាងក្រោម៖

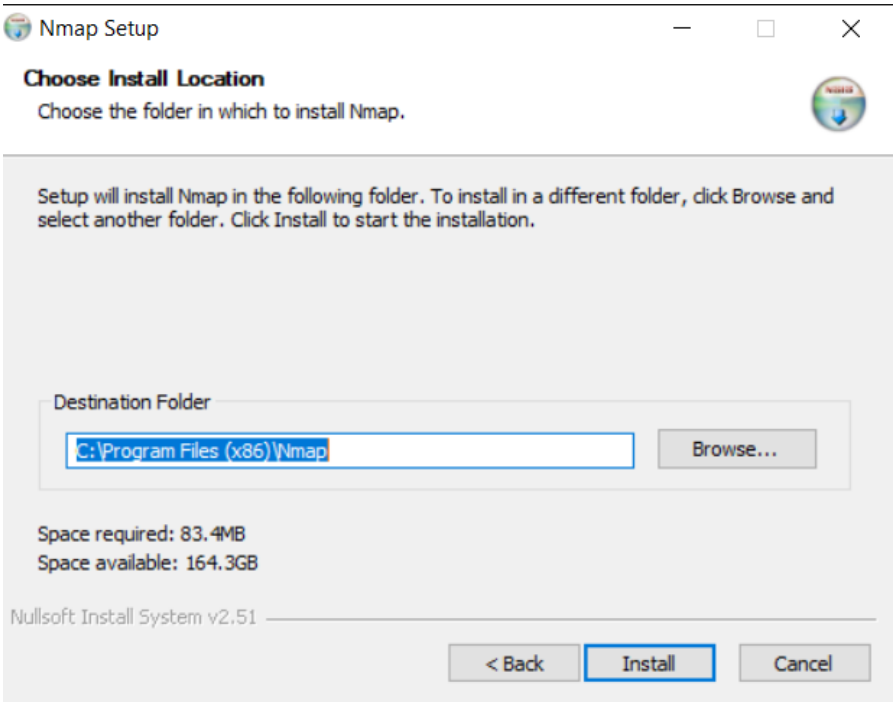
១.ចុចបើកដំណើរការ nmap file ដែលអ្នកបាន download ហើយបន្ទាប់មកចុចពាក្យថា I Agree->Next->Install->Next->Next->Finish ដែលមានបង្ហាញតាមលំដាប់លំដោយដូចរូបខាងក្រោមនេះ៖



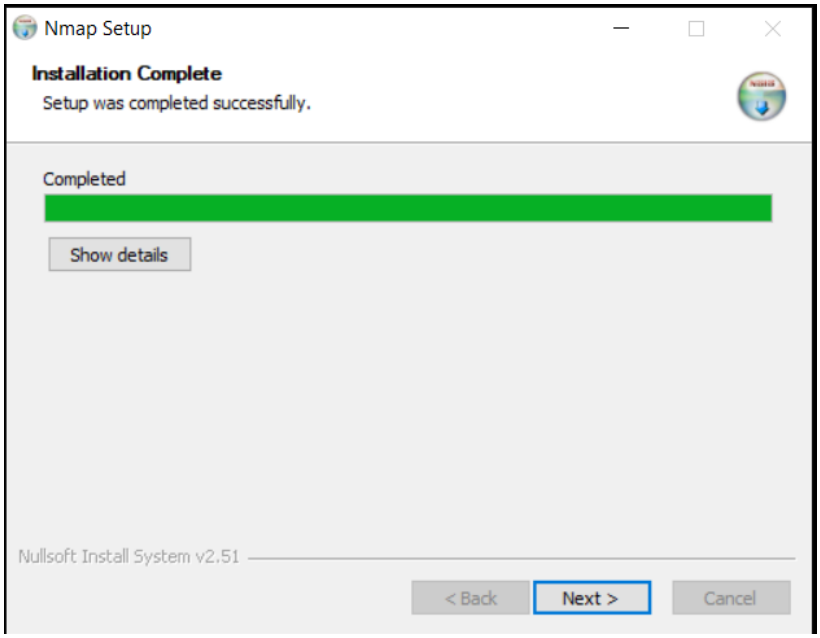
រូបភាពទី ៧៤៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



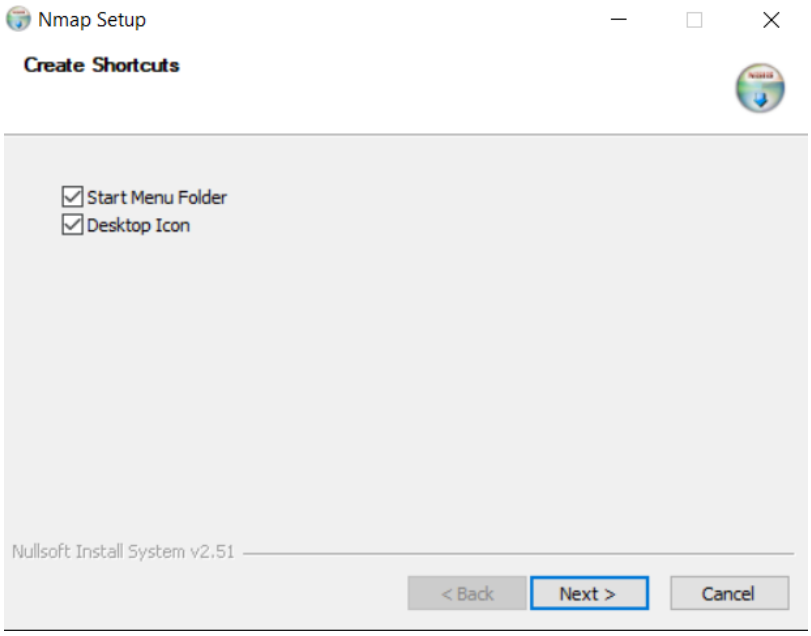
រូបភាពទី ៧៥៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



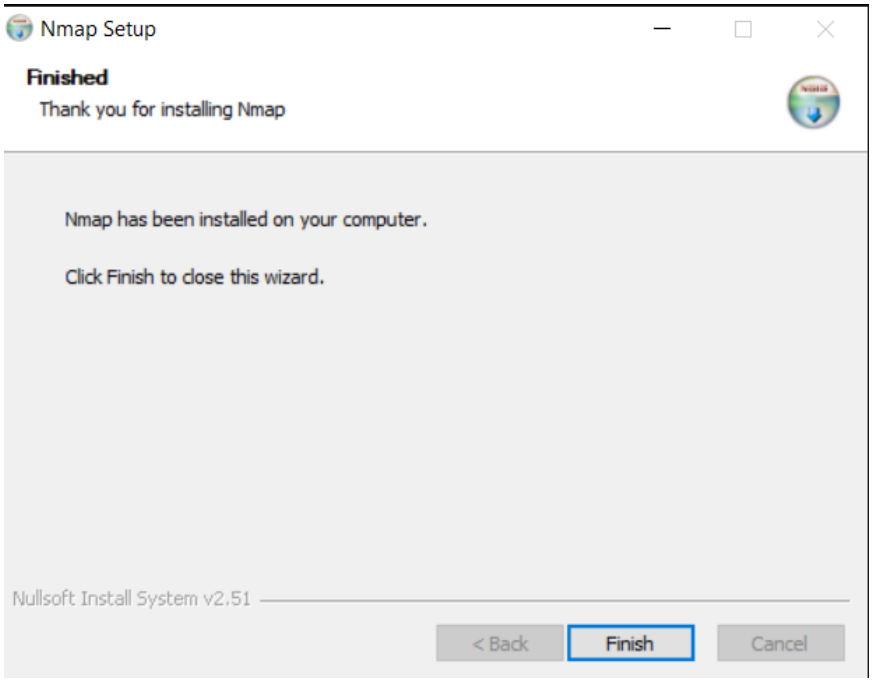
រូបភាពទី ៧៦៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



រូបភាពទី ៧៧៖ បង្ហាញពីការ Install Nmanp នៅលើ Window



រូបភាពទី ៧៨៖ បង្ហាញពីការ Install Nmanp នៅលើ Window

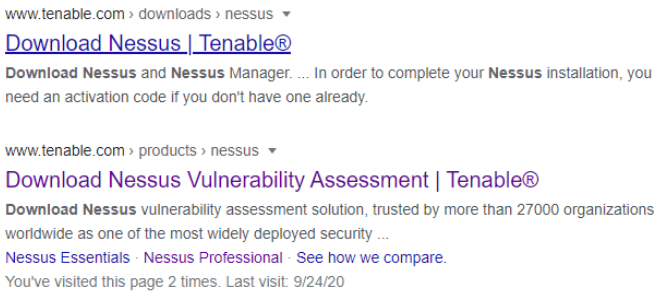


រូបភាពទី ៧៩៖ បង្ហាញពីការ Install Nmanp នៅលើ Window

៣.៤.២. របៀបតំឡើងសូហ្វ៊ែ Nessus

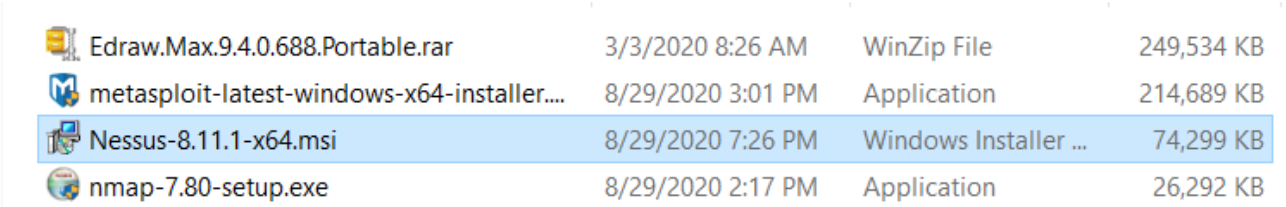
ដើម្បីធ្វើការសាកល្បងណែតវ៉ឺករបស់យើងថាតើមាន សុវត្ថិភាពឬមួយមិនមាន យើងអាចប្រើប្រាស់នូវ សូហ្វ៊ែ Nessus ។ ដូចនេះដើម្បីប្រើប្រាស់នូវ សូហ្វ៊ែនេះបានយើងគួរដំឡើងវា តាមដំណាក់ដូចខាងក្រោម៖

១. ដំបូងយើងត្រូវចូលទៅក្នុង Web Browser រួចវាយពាក្យ Download Nessus



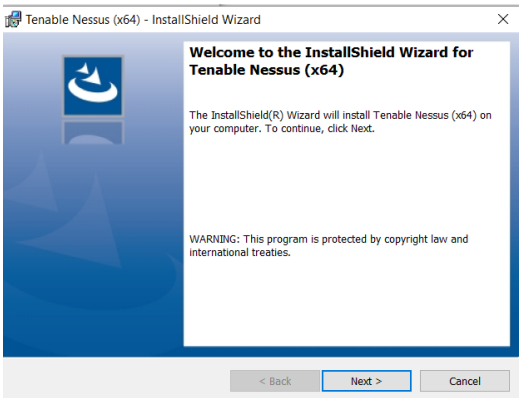
រូបភាពទី ៨០៖ បង្ហាញអំពីការដោតទ្បូត សូហ្វ៊ែ Nessus

២. បន្ទាប់ពីយើងទទួលបានហើយ យើងចុចពីរដងទៅ Software Nessus



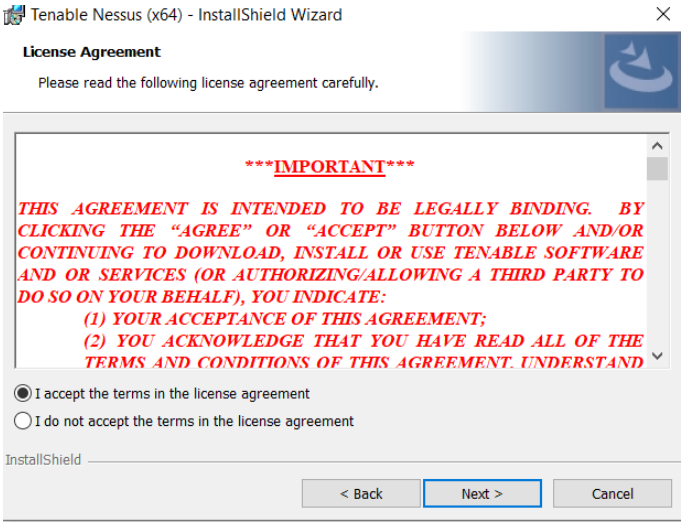
រូបភាពទី ៨១ ៖ បង្ហាញអំពី File Of Nessus

៣. បន្ទាប់មកយើងចុចពាក្យថា Next



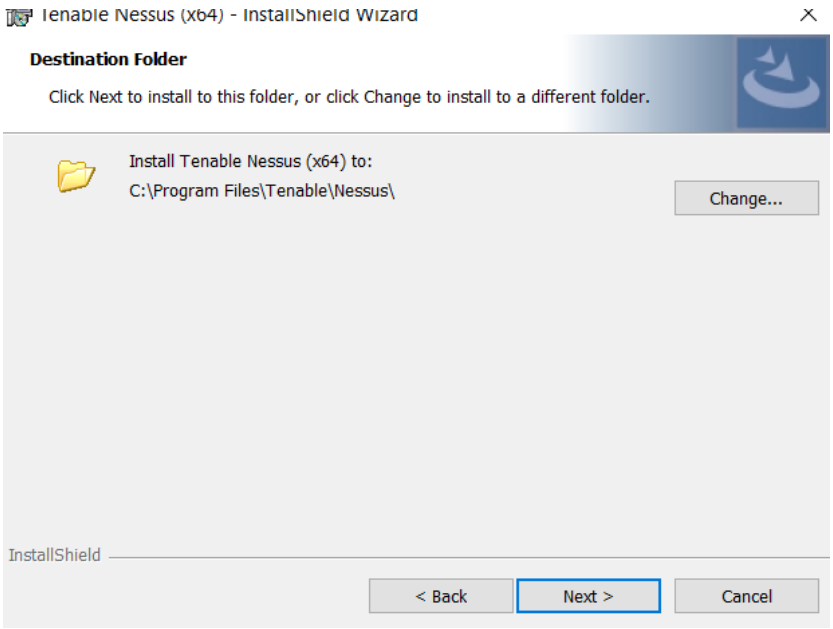
រូបភាពទី ៨២៖ បង្ហាញអំពីការដោតទ្បូត សូហ្វ៊ែ Nessus

៤. បន្ទាប់មកយើងចុចពាក្យថា I Accept the Term in the License Agreement



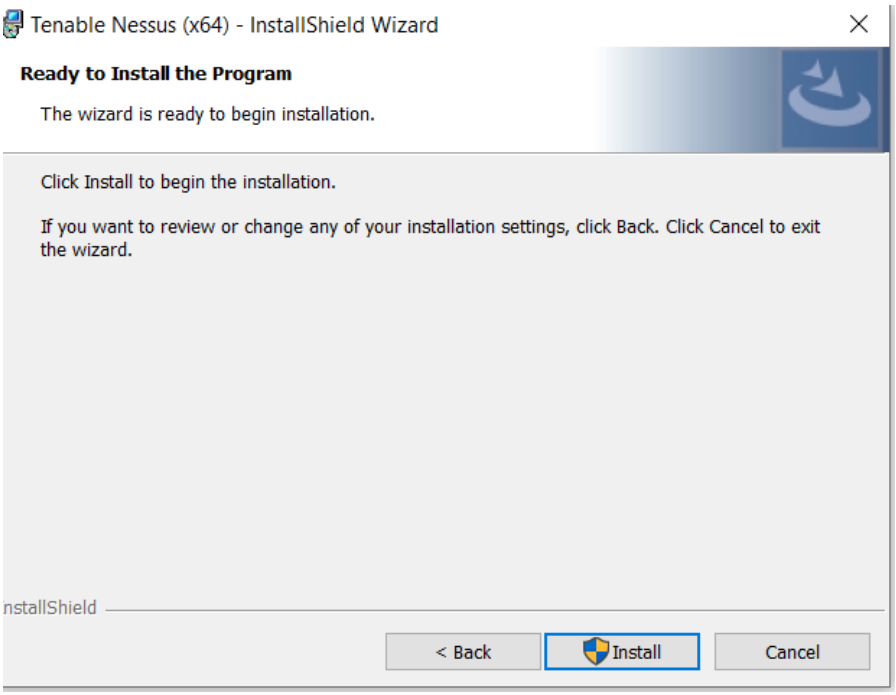
រូបភាពទី ៨៣ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

៥. បន្ទាប់មកយើងចុចពាក្យថា Next



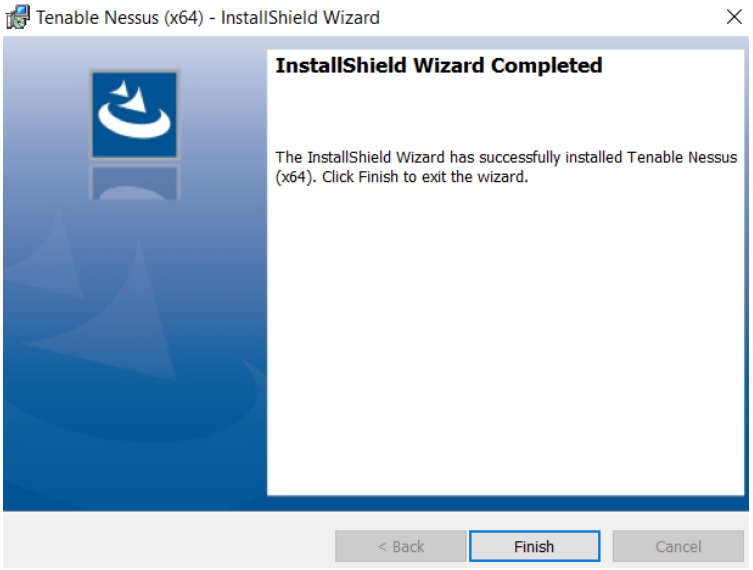
រូបភាពទី ៨៤ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

៦. បន្ទាប់មកយើងចុចពាក្យថា Install



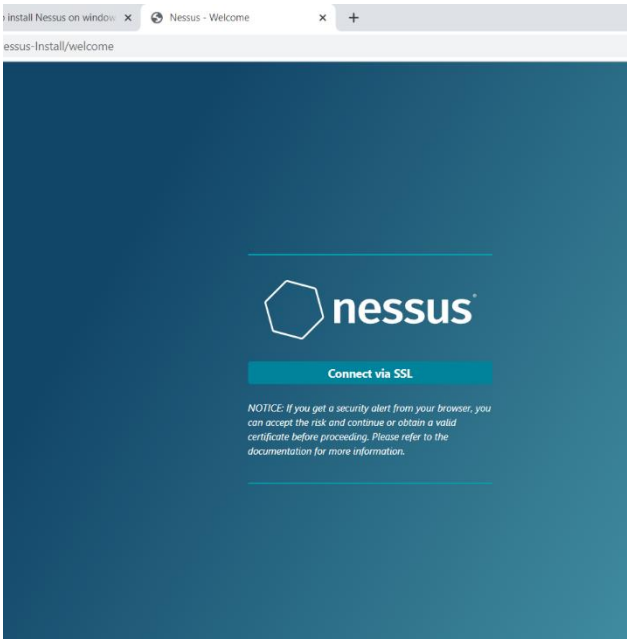
រូបភាពទី ៨៥ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

៧. បន្ទាប់មកយើងចុចពាក្យថា Finish



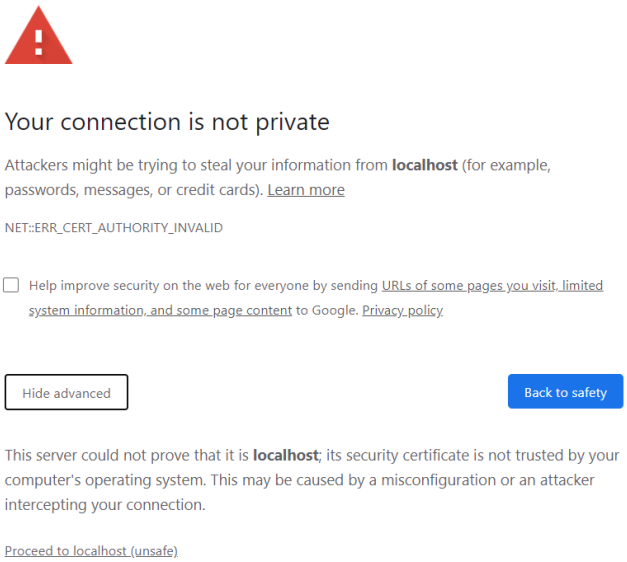
រូបភាពទី ៨៦ ៖ បង្ហាញអំពីការព្រមនៃការដោតឡូត សូហ្វ៊ែ Nessus

៨. បន្ទាប់មកវានឹងលោតផ្ទាំង Nessus នៅលើ Web Browser រួចចុច Connected Via SSL



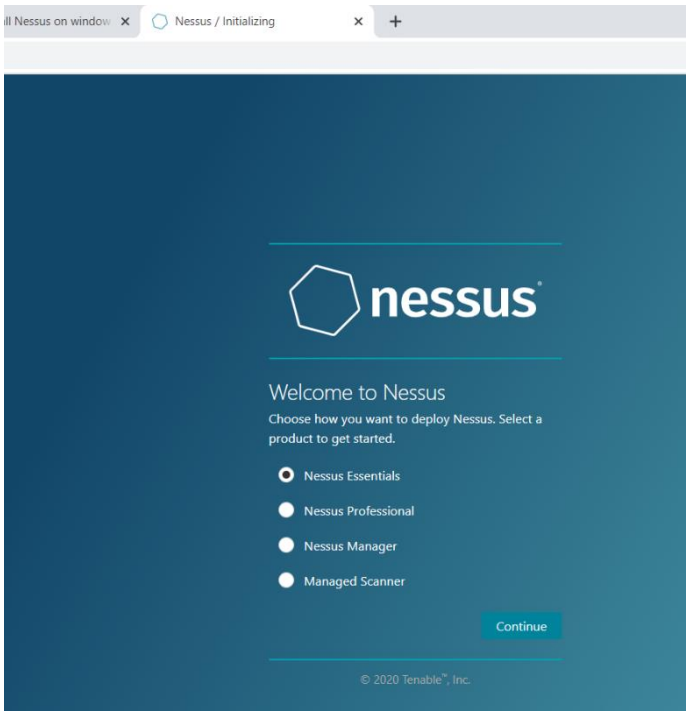
រូបភាពទី ៨៧ ៖ បង្ហាញអំពីផ្ទាំង សូហ្វ៊ែ Nessus នៅក្នុង Web Browser

៩. បន្ទាប់មកយើងចុចលើ Processed in Localhost



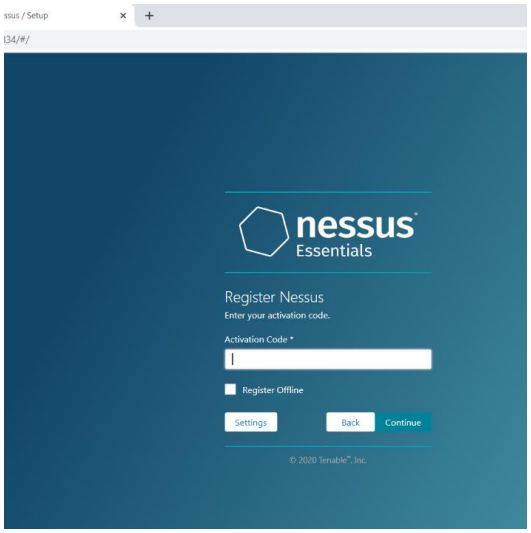
រូបភាពទី ៨៨ ៖ បង្ហាញអំពីផ្ទាំង Processed to LocalHost

១០. បន្ទាប់មកជ្រើសរើពាក្យ Nessus Essentials រួចចុចពាក្យ Next



រូបភាពទី ៨៩ ៖ បង្ហាញអំពីការជ្រើសរើស Nessus Essential

១១. បន្ទាប់មកយើង Register Code រួចចុចពាក្យថា Next

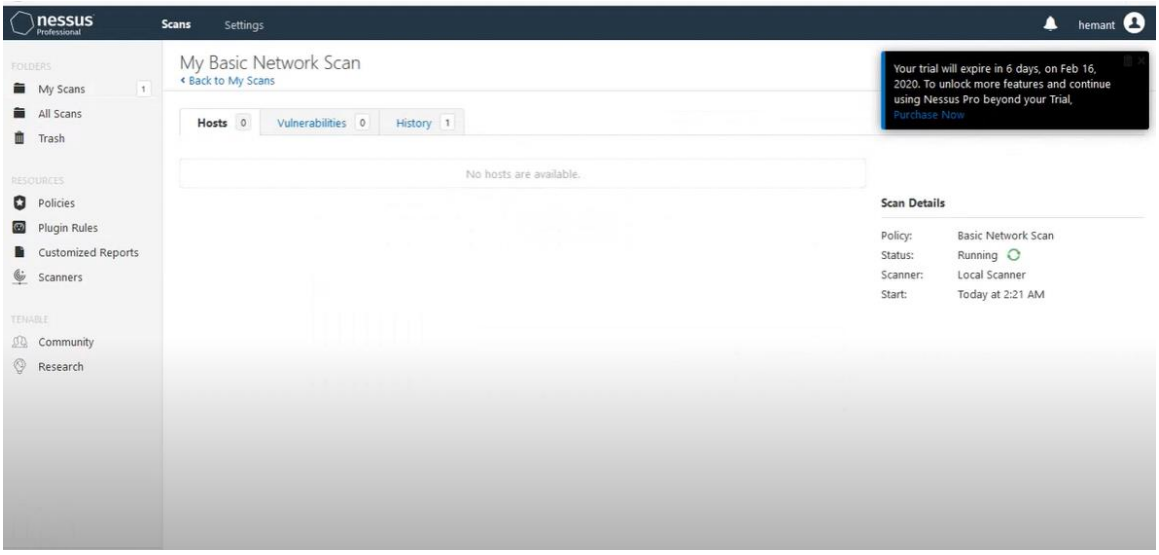


រូបភាពទី ៩០ ៖ បង្ហាញអំពីការវាយ Register Nessus

១២. រួចយើងវាយ Username នឹង Password

រូបភាពទី ៩១ ៖ បង្ហាញអំពីការវាយ Username & Password

១៣. បន្ទាប់មកវានឹងលោតផ្ទាំងនៅក្នុង Nessus



រូបភាពទី ៩២ ៖ បង្ហាញអំពីផ្ទាំងនៃការស្វែងរក Nessus Scan

សេចក្តីសន្និដ្ឋាន និង ការផ្តល់អនុសាសន៍

១. សេចក្តីសន្និដ្ឋាន

ក្រោយពីបានសិក្សាអំពីមុខវិជ្ជាសេដ្ឋកិច្ចព័ត៌មានវិទ្យាកន្លងមក យើងបានដឹងថាវាពិតជាមានសារៈប្រយោជន៍ណាស់ចំពោះមនុស្សទូទៅ។ សម័យបច្ចុប្បន្នវិទ្យាសាស្ត្រគឺកាន់តែមានការរីកចម្រើនឥតឈប់ឈរ ជាពិសេស ជាពិសេសគឺ វិស័យបច្ចេកវិទ្យាព័ត៌មាន ដែលត្រូវបានគេបានកំពុងអភិវឌ្ឍន៍នានា យើងសង្កេតឃើញថាវិស័យបច្ចេកវិទ្យាព័ត៌មានកុំព្យូទ័រ កំពុងត្រូវបានយកចិត្តទុកដាក់យ៉ាងខ្លាំង ព្រោះវាជាកត្តាចំបងក្នុងការអភិវឌ្ឍប្រទេសជាតិ ឲ្យមានការរីកចម្រើនឡើងទៅតាមការផ្លាស់នៃសម័យទំនើប ។ ដើម្បីធ្វើឲ្យប្រព័ន្ធណែតវឺក មានដំណើរការបានល្អ និងសុវត្ថិភាព ហើយងាយស្រួលក្នុងការគ្រប់គ្រង ត្រូវប្រើប្រាស់នូវឧបករណ៍ទាន់សម័យទៅតាមសង្គមយើងបច្ចុប្បន្ន កុំព្យូទ័រ ជាពិសេស ផ្នែករឹងនៃកុំព្យូទ័រ ឲ្យមានល្បឿនខ្ពស់ និងការជ្រើសរើសទីតាំងនៃបរិស្ថានជុំវិញឲ្យមានសុវត្ថិភាពខ្ពស់ ថែមទាំងអាចធ្វើការទំនាក់ទំនងគ្នាបានថែមទៀតផងដែលលក្ខណៈបែបនេះ គេហៅថា ប្រព័ន្ធណែតវឺក ៖

- សម្រួលដល់កិច្ចការផ្សេងៗ ក្នុងដំណើរការទំនាក់ទំនងគ្នាប្រចាំថ្ងៃ ។
- មានភាពងាយស្រួលទាំងការបញ្ជូន នឹងទទួលព័ត៌មាន ។
- មានភាពងាយស្រួលក្នុងការគ្រប់គ្រង់ឯកសារ នឹងចែកចាយឯកសារ។

ដូច្នេះហើយ បណ្តាញប្រព័ន្ធណែតវឺក ផ្តល់នូវអត្ថប្រយោជន៍យ៉ាងច្រើនដល់មនុស្សទូទៅ គឺវាជួយសម្រួលនូវរាល់កិច្ចការផ្សេងៗ និងការទំនាក់ទំនងយ៉ាងរហ័សទាន់ពេលវេលា ព្រមទាំងផ្តល់នូវសុវត្ថិភាពផងដែរ ។

២. ការផ្តល់អនុសាសន៍

ដើម្បីអោយប្រព័ន្ធណែតវឺកមានដំណើរល្អ និងផ្តល់ភាពងាយស្រួលដល់អ្នកប្រើប្រាស់ យើងគួរតែមានការបន្ថែមនូវវិធីសាស្ត្រ ដើម្បីធ្វើការរៀបចំ និងធ្វើការពារចំពោះកុំព្យូទ័រនៅក្នុងប្រព្ធន័ណែតវឺកដូចជា៖

- ធ្វើការ update នៃ software នៃកម្មវិធីប្រើប្រាស់ប្រចាំថ្ងៃ ។
- បើកដំណើរការរបស់ Firewall របស់កុំព្យូទ័រ ។

ឯកសារយោង

ឯកសារយោង

១. សៀវភៅ របាយការណ៍កម្មសិក្សា ការការពារប្រព្ធន័ណែតវឺក ចងក្រងដោយនិស្សត សៀង ពិសិទ្ធ និង ជូរ ឈុនហ៊ីម នៃសាកលចិទ្យាល័យ ភូមិន្ទនីតិសាស្ត្រ និងវិទ្យាសាស្ត្រសេដ្ឋកិច្ច ។

២. https://searchnetworking.techtarget.com/definition/WAN-wide-area-network

៣.https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

៤. https://www.guru99.com/tcp-ip-model.html

៥. https://privacy.net/how-to-secure-your-computer/

៦. https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

៧. https://www.barracuda.com/glossary/network-firewall

៨.https://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

៩.https://www.itsupportguides.com/knowledge-base/windows-10/windows-defender-smartscreen-prevented-an-unrecognized-app-error/

១០.https://techcommunity.microsoft.com/t5/windows-insider-program/windows-defender-application-guard-standalone-mode/m-p/66903

១១.https://www.howtogeek.com/howto/windows-vista/disable-user-account-control-uac-the-easy-way-on-windows-vista/

១២.https://www.microsoft.com/security/blog/2017/10/23/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/

១៣.https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard

១៤.https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

១៥.https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

១៦. https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption

ว ฦ .//https://itcambonews.wordpress.com/2016/05/10/%E1%9E%94%E1%9F%92%E1%9E%9A%E1%9E%96%E1%9F%90%E1%9E%93%E1%9F%92%E1%9E%92%E1%9E%80%E1%9E%BB%E1%9F%86%E1%9E%96%E1%9F%92%E1%9E%99%E1%9E%BC%E1%9E%91%E1%9F%90%E1%9E%9A-%E1%9E%8E%E1%9F%82%E1%9E%8F%E1%9E%9C/