Mencegah Penyebaran Ransomware Wannacry di Windows

Beberapa hari terakhir Ransomware wannacry telah menghebohkan dunia IT dan telah masuk di lebih dari 99 negara, termasuk di Indonesia. **Ransomware** adalah salah satu jenis **malware** yang bertujuan untuk meminta tebusan kepada korban. Ransomware, sesuai dengan namanya, *ransom* = tebusan (dalam bahasa Inggris), jenis malware ini bertujuan untuk memeras korban yang komputernya terinfeksi ransomware dengan meminta sejumlah uang sebagai tebusan.

Berikut ini adalah beberapa extensi file yang menjadi target dari Malware Ransomware Wannacrypt :

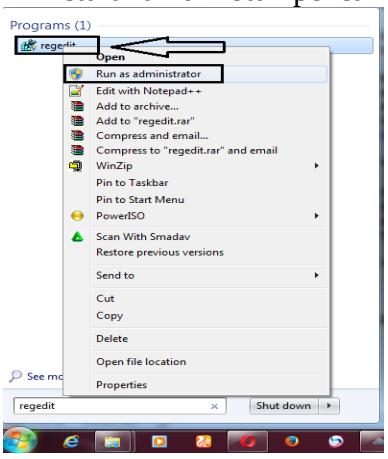
- Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
- Less common and nation-specific office formats (.sxw, .odt, .hwp).
- Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
- Emails and email databases (.eml, .msg, .ost, .pst, .edb).
- Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
- Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
- Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
- Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
- Virtual machine files (.vmx, .vmdk, .vdi).

Berikut ini adalah beberapa tindakan pencegahan untuk meminimalisir terinfeksi Malware Ransomware Wannacrypt atau wannacry:

1. **Jangan terkoneksi di LAN/WIFI & Lakukan Back Up Data**
2. **Lakukan Update AntiVirus**
3. **Lakukan Update Patch MS17-010 pada OS Windows**
   Untuk update patch windows dapat di download di :
   http://openstorage.gunadarma.ac.id/wannacry/

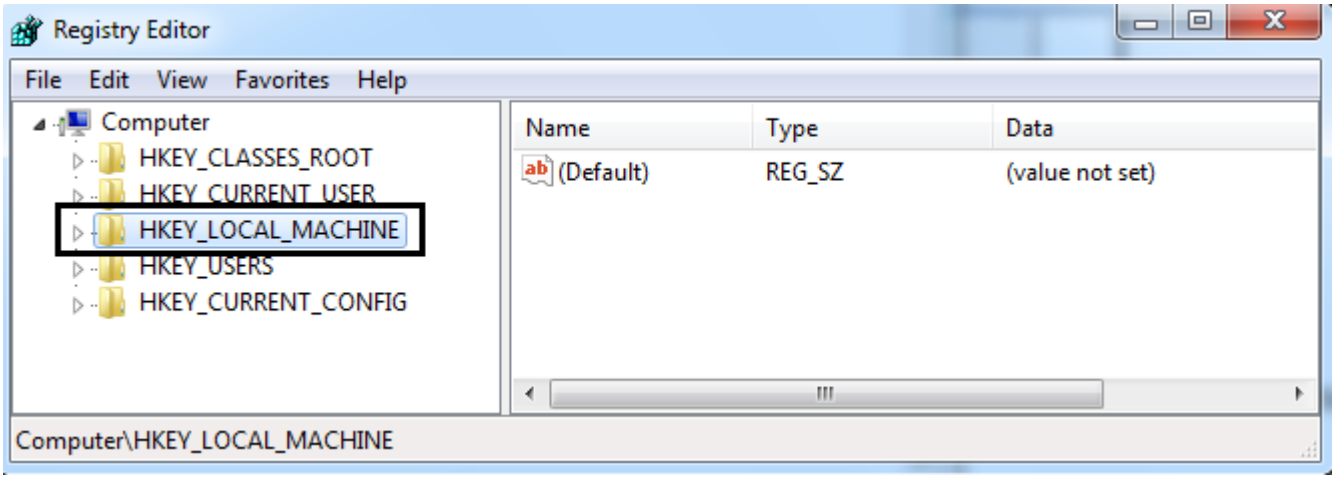
4. **Non Aktifkan Fungsi SMB v1 & SMB v2**
   Server Message Block disingkat SMB adalah protokol standar yang dibuat oleh Microsoft yang digunakan pada sistem windows. Fungsi SMB dalam windows adalah sebagai protokol yang digunakan untuk membagi data (sharing file), baik dari perangkat CD-ROM, harddisk, maupun perangkat output seperti printer untuk dapat digunakan bersama-sama.

   Cara Mematikan fitur SMB V1 untuk windows 7
   Klik start-run di kotak pencarian ketikan regedit – run as administrator – lalu klik ok

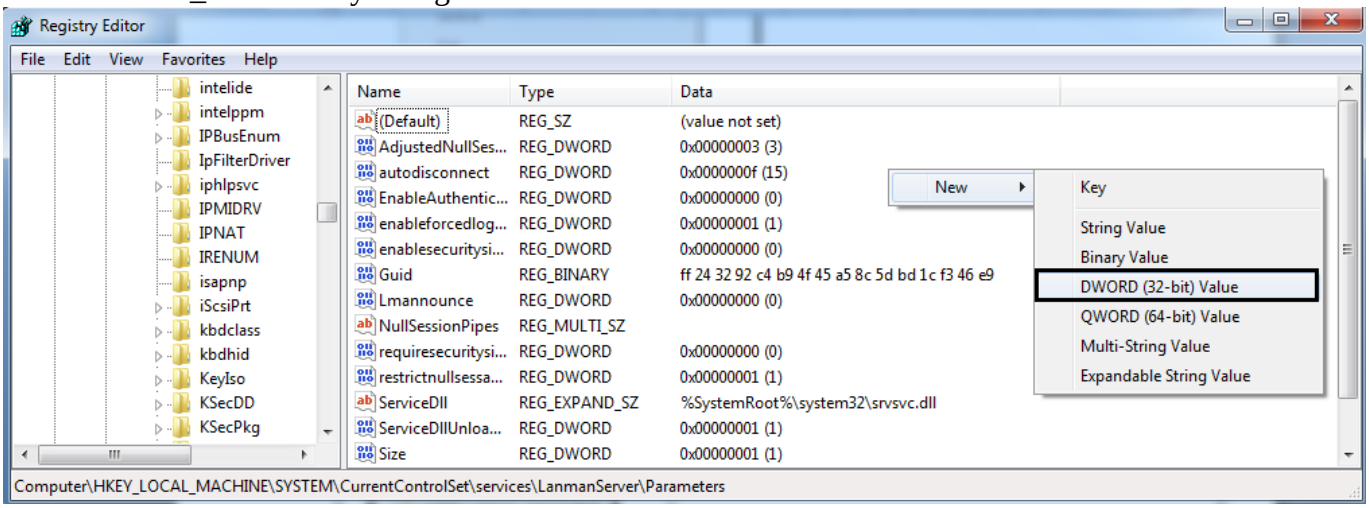


Langsung saja kita pergi ke PATH

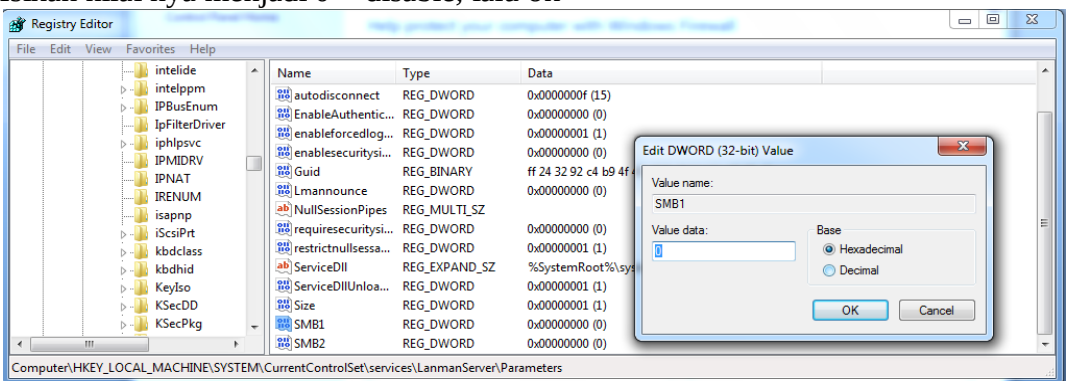
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters



Kita buat REG_DWORD nya dengan nama SMB1 & SMB2



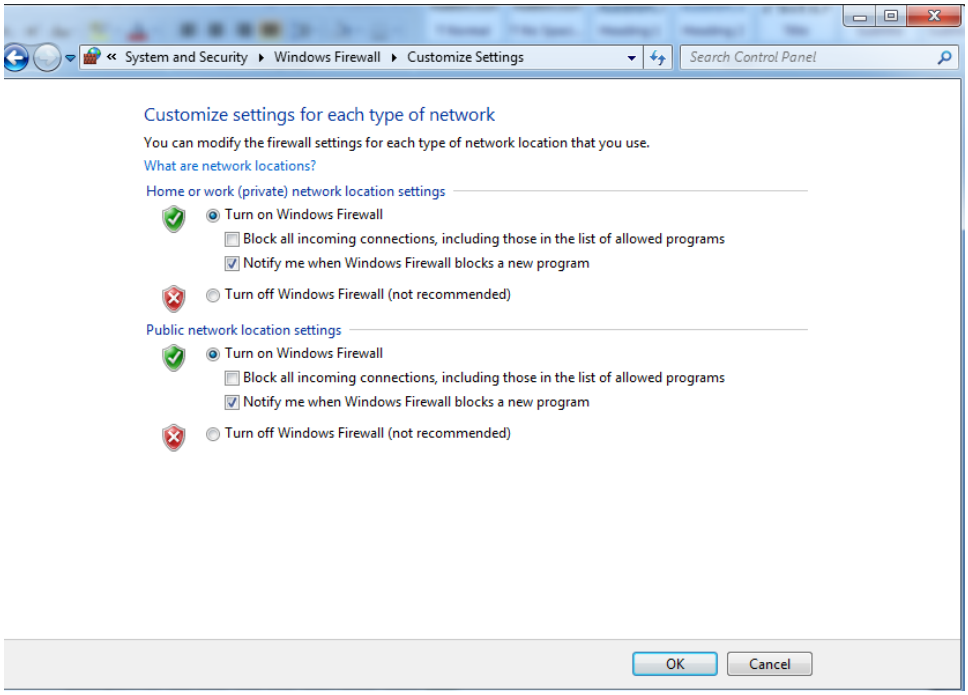
Isikan nilai nya menjadi 0 = disable, lalu ok



Setelah semua konfigurasi udah selesai di buat jangan lupa untuk merestart windows anda.

5. **Aktifkan firewall di windows control panel**

   Control panel – System and Security – Windos Firewall – Customize Settings



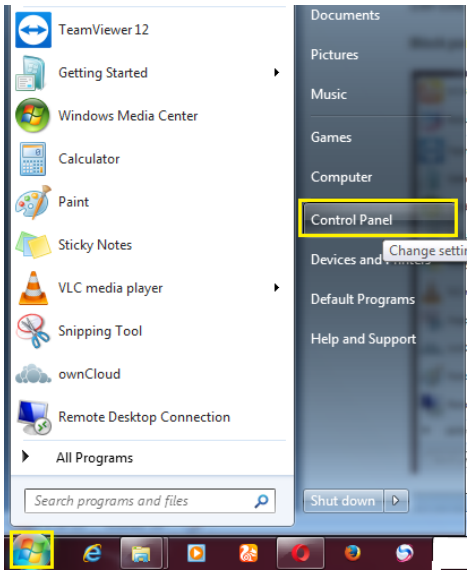
6. **Blokir port TCP & port UDP yang di gunakan sebagai media Wannacry yaitu port** 135-139, 445, 3389

   Tambahkan juga port lainnya seperti port 135-139, 445, 593, 1024-1030, 3389, 4444

   Block port TCP 135-139, 445, 593, 1024-1030, 3389, 4444

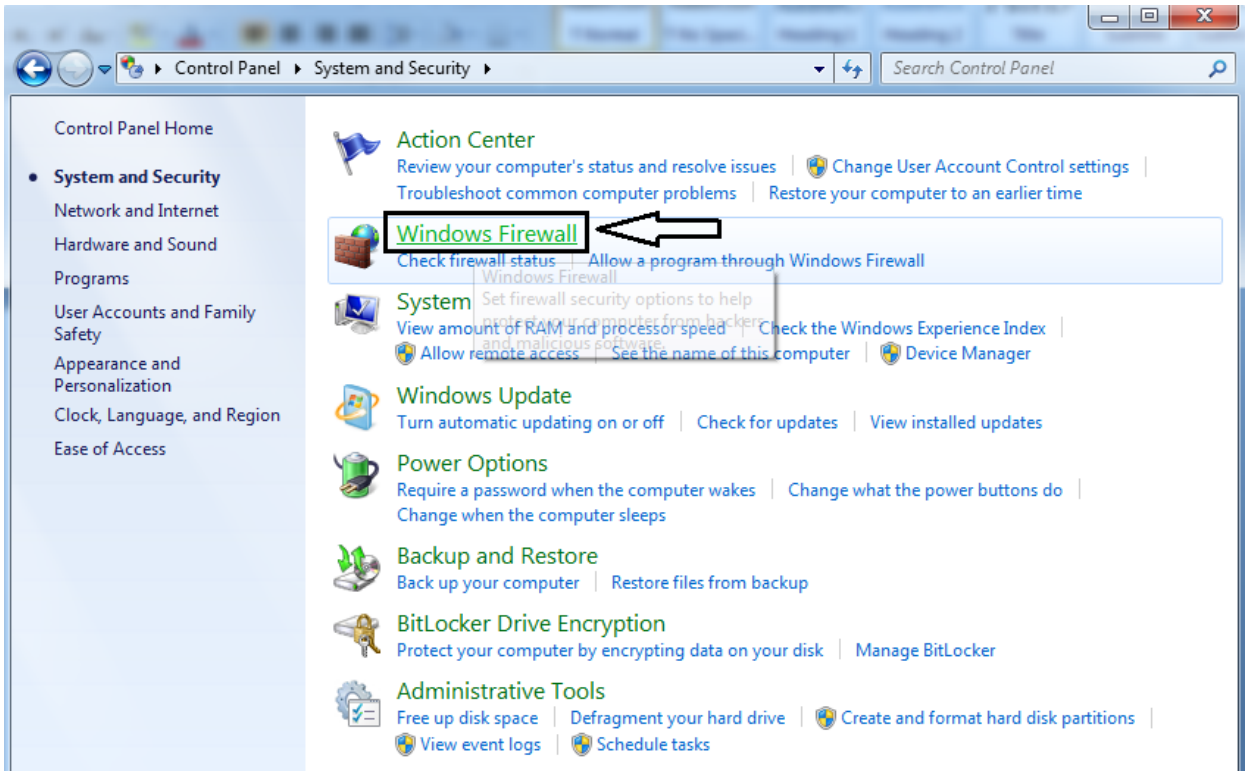
   Untuk memblok nya kita perlu mengaturnya di contol panel windows anda.

   Start – Control Panel

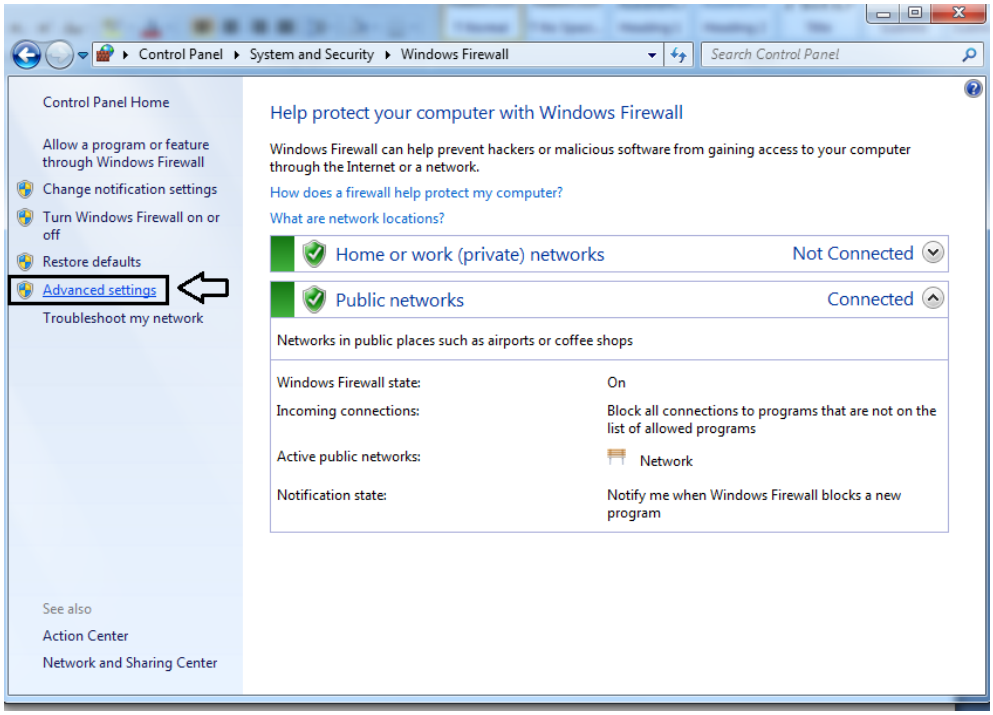


System and Security

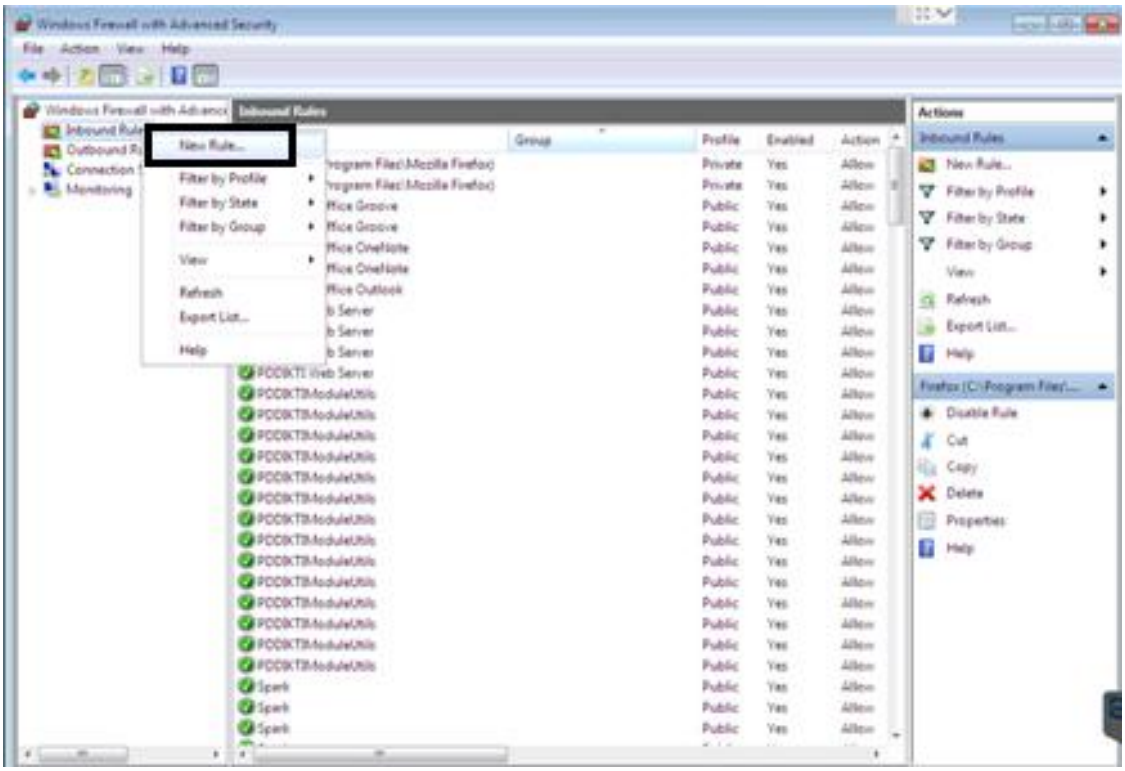
Windows Firewall



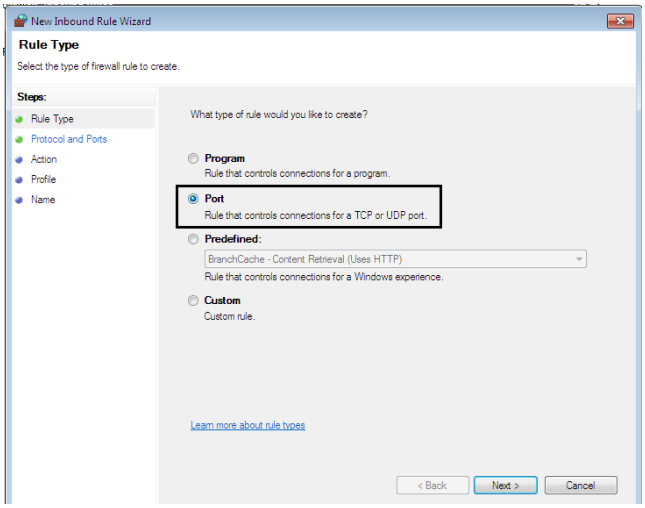
Advanced settings



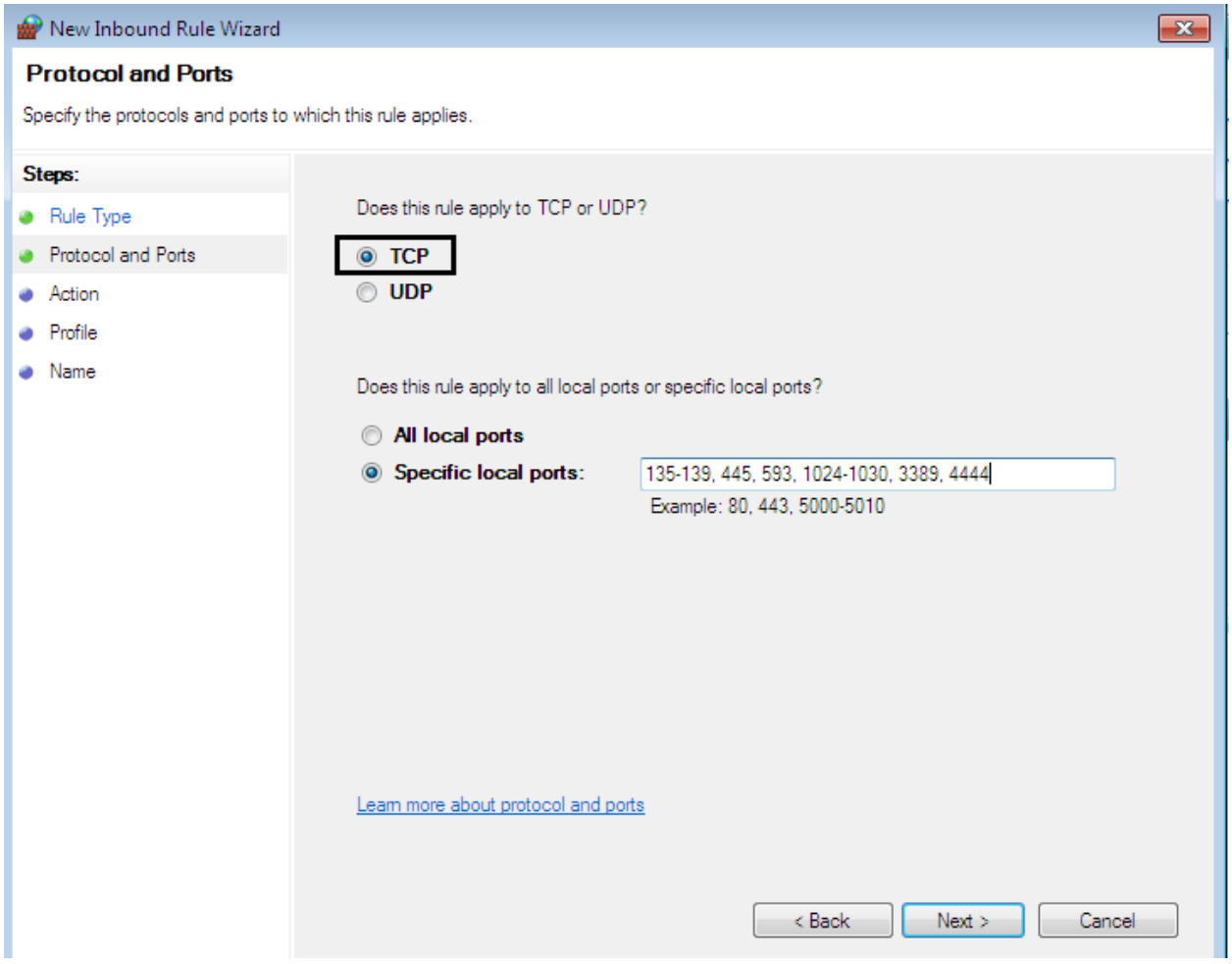
Klik kanan pada Inbound Rules – New Rule



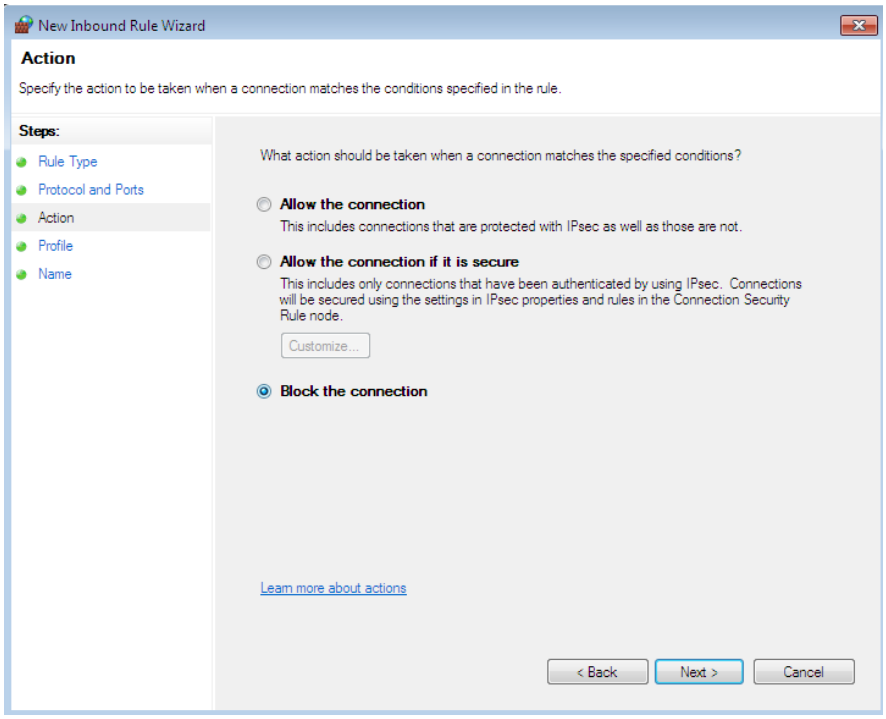
Lalu checklist Port => klik Next



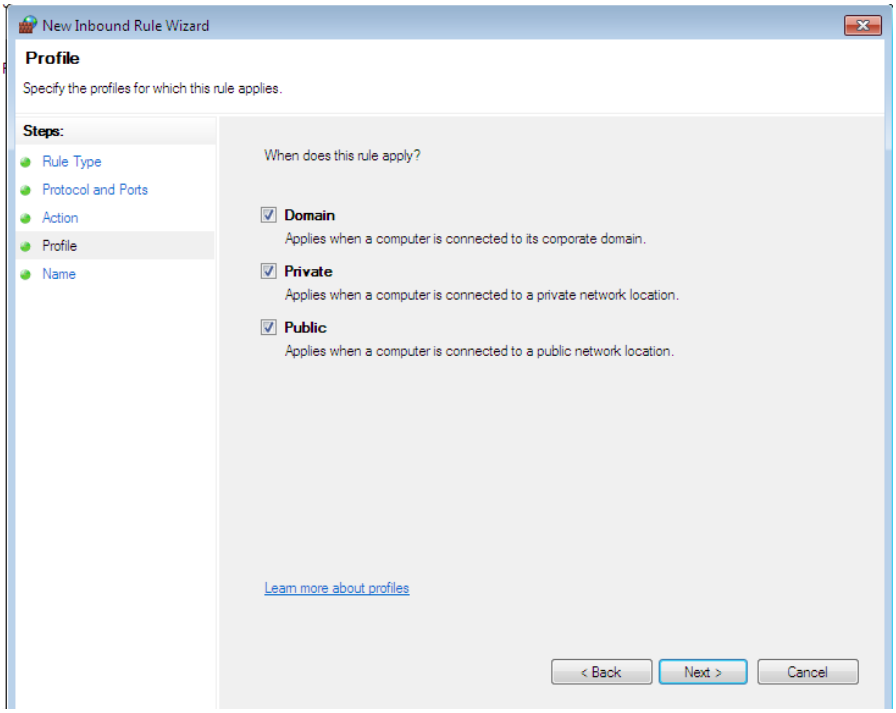
Checklist => TCP
Checklist => Specific local ports, isikan : 135-139, 445, 593, 1024-1030, 3389, 4444
Klik Next



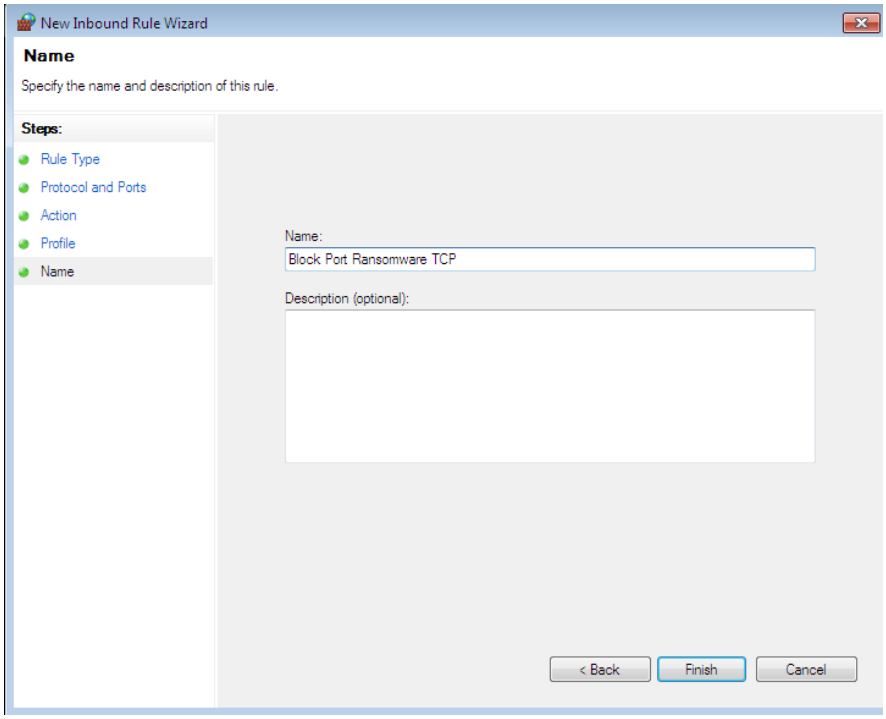
Checklist => Block the connection, next



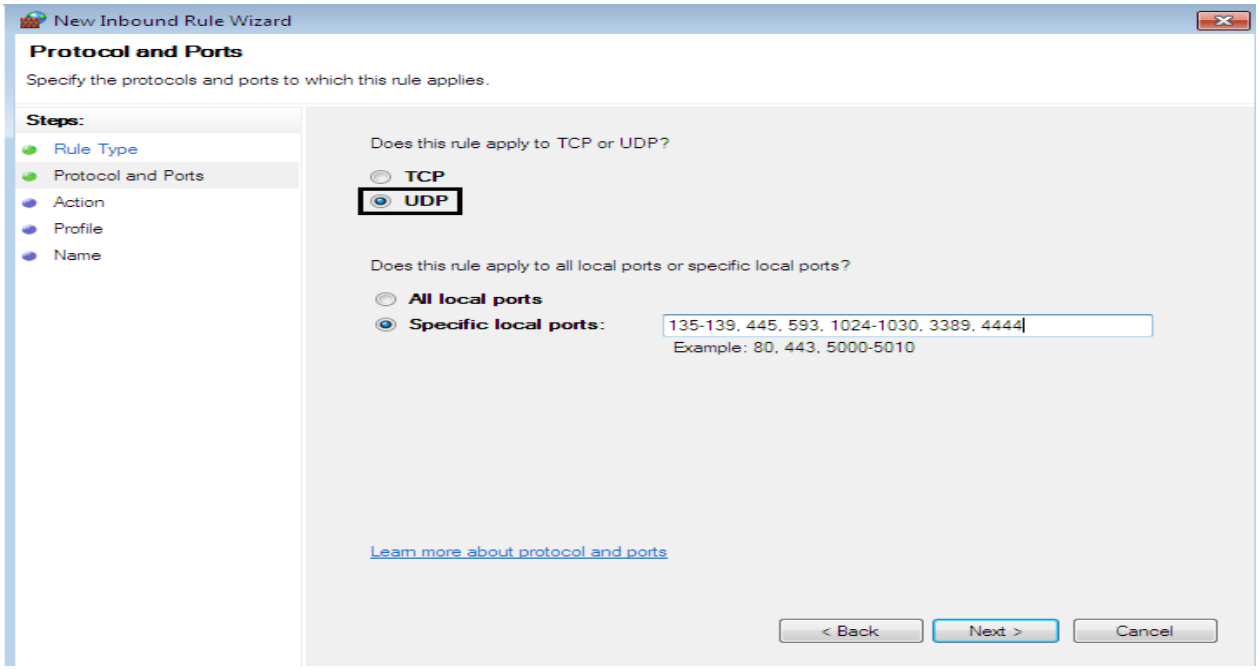
Checklist => Domain, Private & Public. next



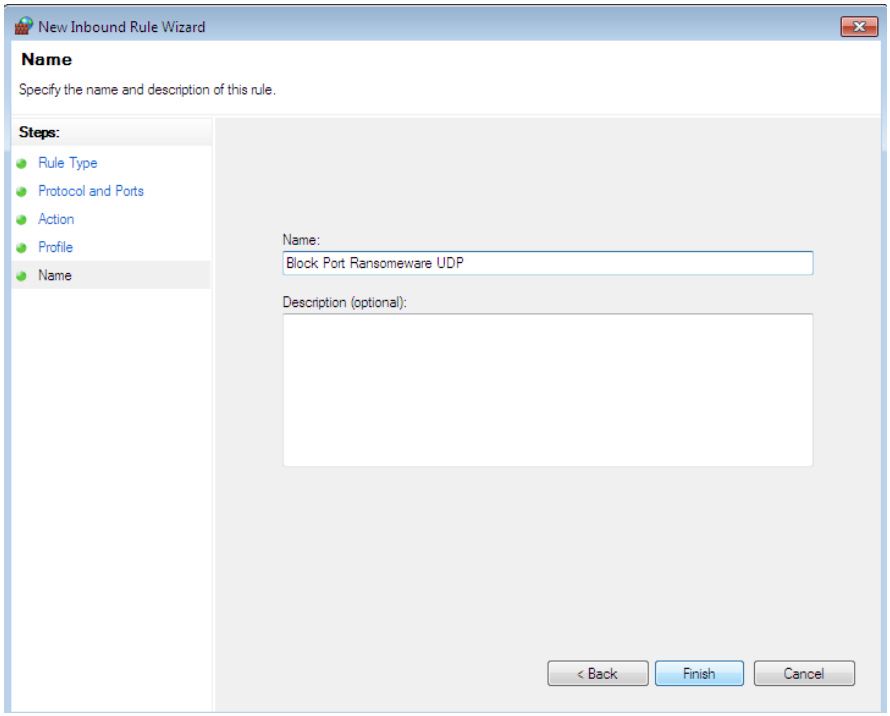
Isikan profile nama nya = Block Port Ransomware TCP, lalu klik finish



Untuk memblok port UDP sama langkahnya memblock port TCP yang baru kita buat di atas, hanya yang membedakan pada **Protocol and Ports** kita checklist => **UDP**



Dan buat profil nama nya => Block Port Ransomware UDP



Selesai & Selamat Mencoba !!!