

AVG AntiVirus Free

1 Notifications

Menu

We're protecting you on this network

Firewall is protecting you by blocking connections from other computers, printers, and devices on the untrusted network you're connected to. [Ignore message](#)

OPEN FIREWALL

BASIC PROTECTION

FULL PROTECTION

Computer

Protected

Web & Email

Protected

Hacker Attacks

Not Protected

Personal Data

Not Protected

YOU'RE UP TO DATE

Last updated: 34 minutes ago

RUN SMART SCAN

RUN OTHER SCANS

Last virus scan: 5 days ago

AVG AntiVirus Free

1 Notifications

Menu

Enhanced Firewall

Apps

Networks

Logs

Premium

ACTIVE 10

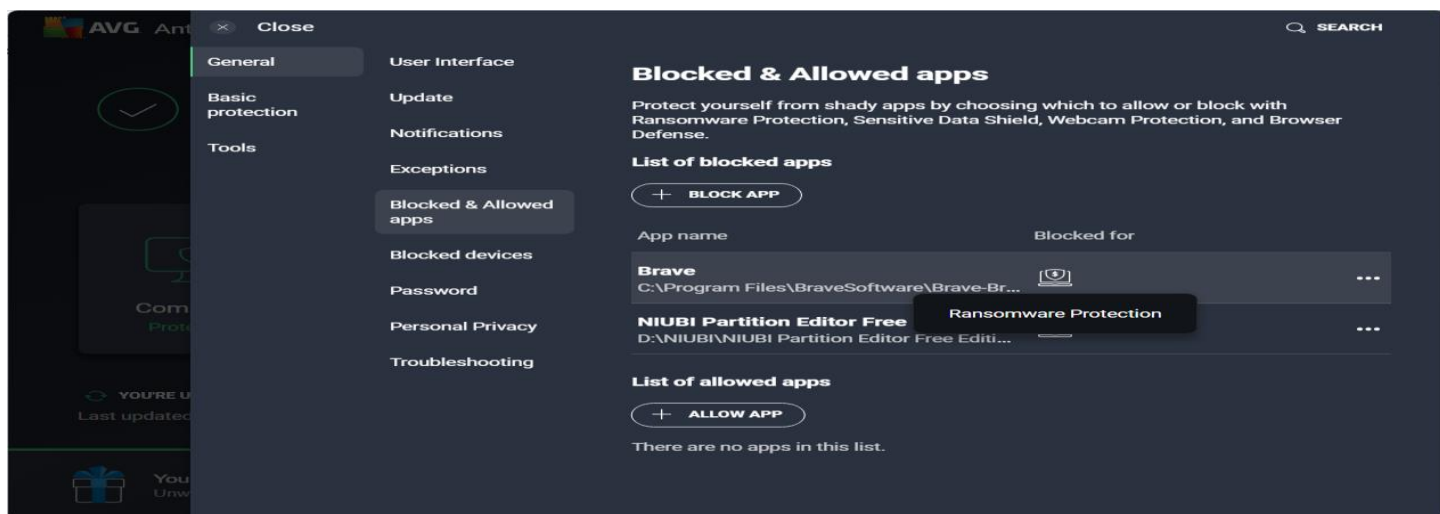
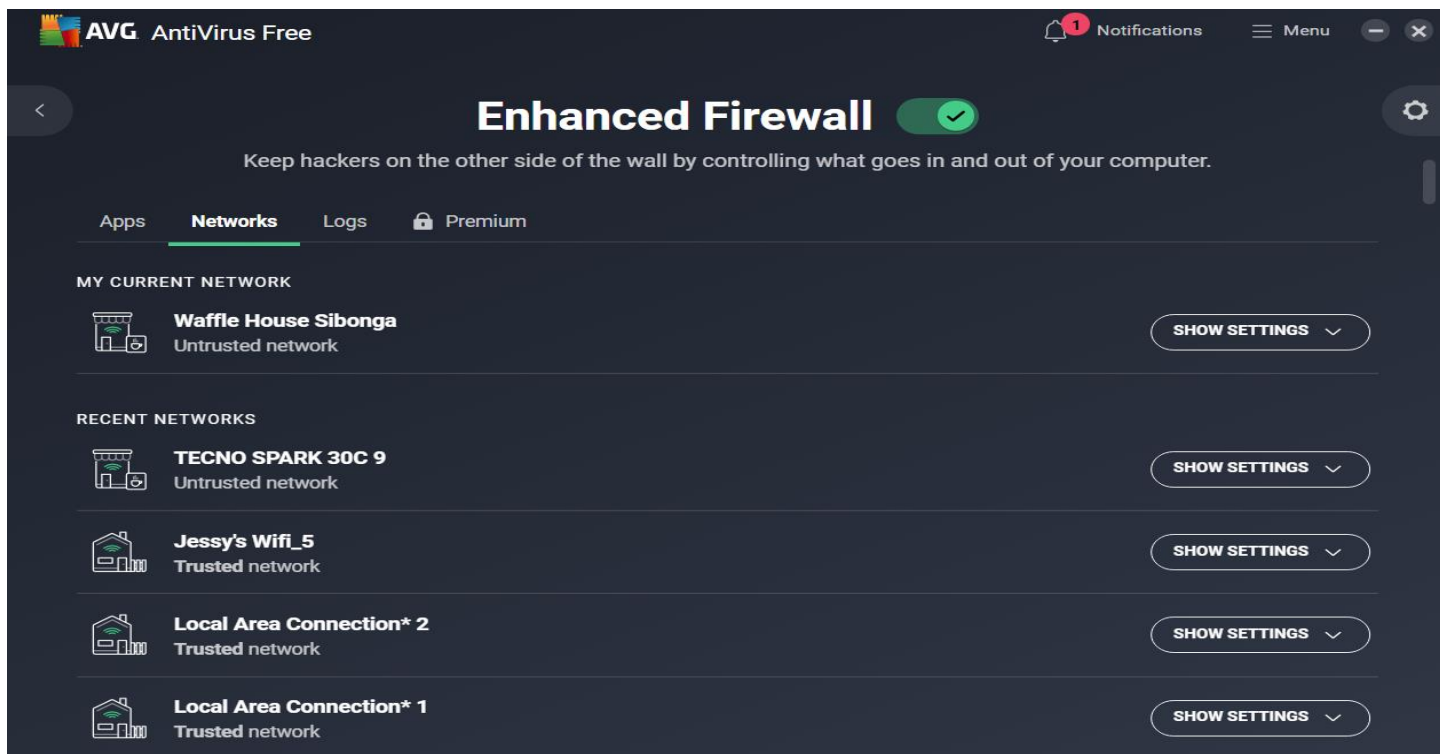
INACTIVE 94

BLOCKED 0

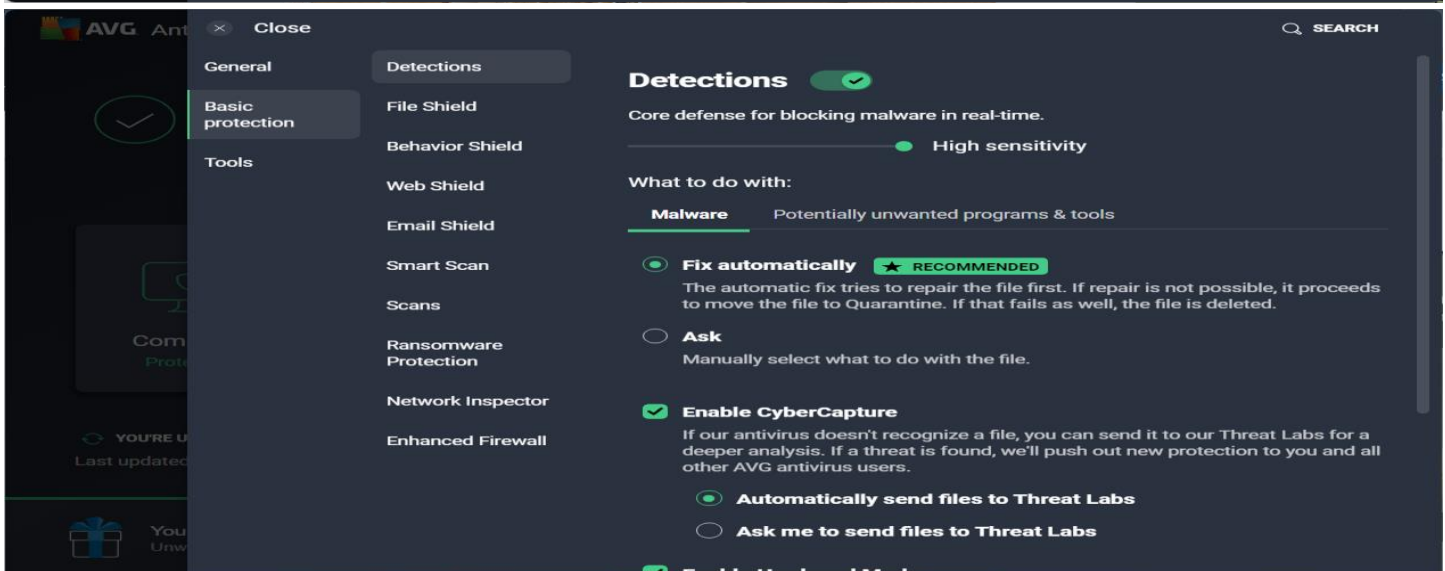
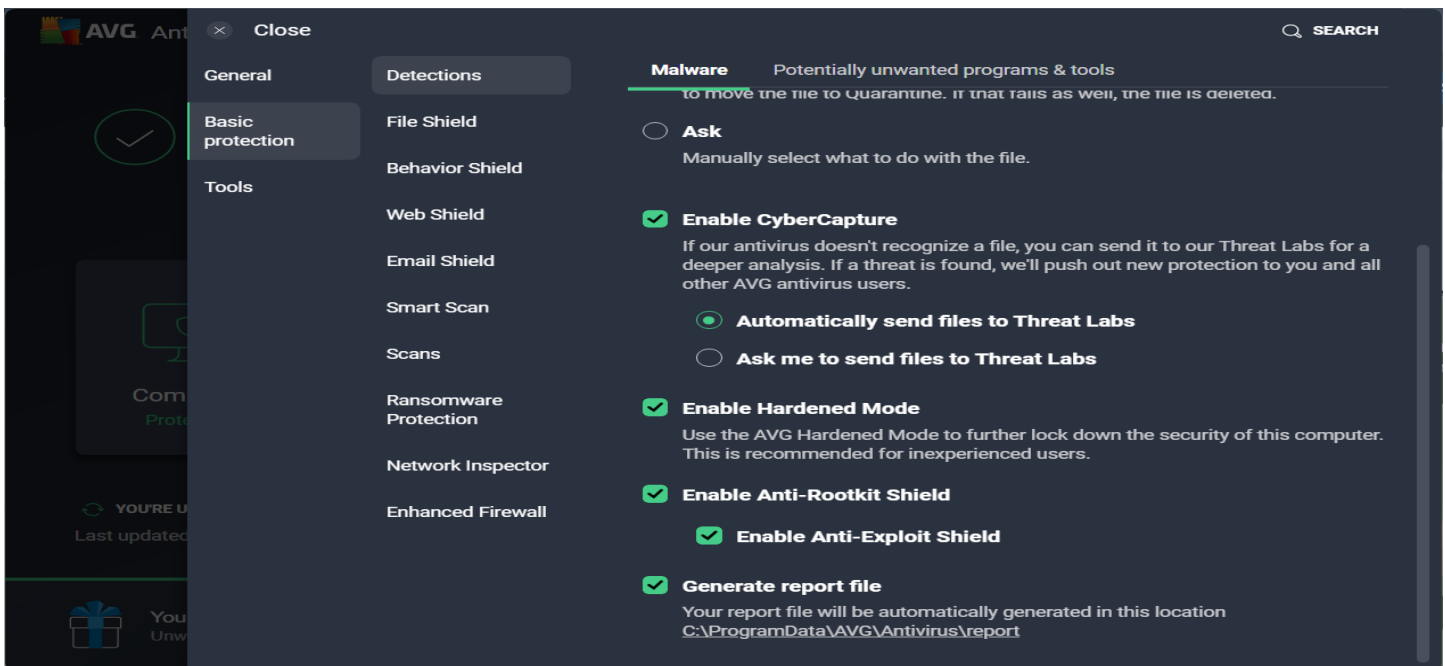
ALL 104

MORE

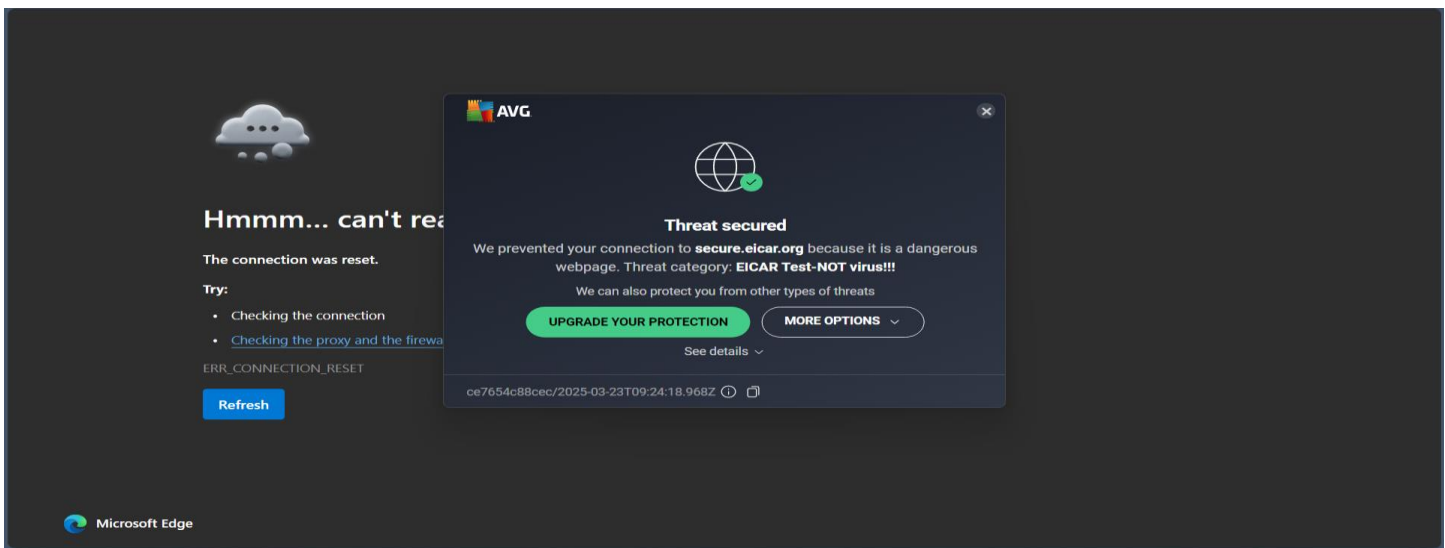
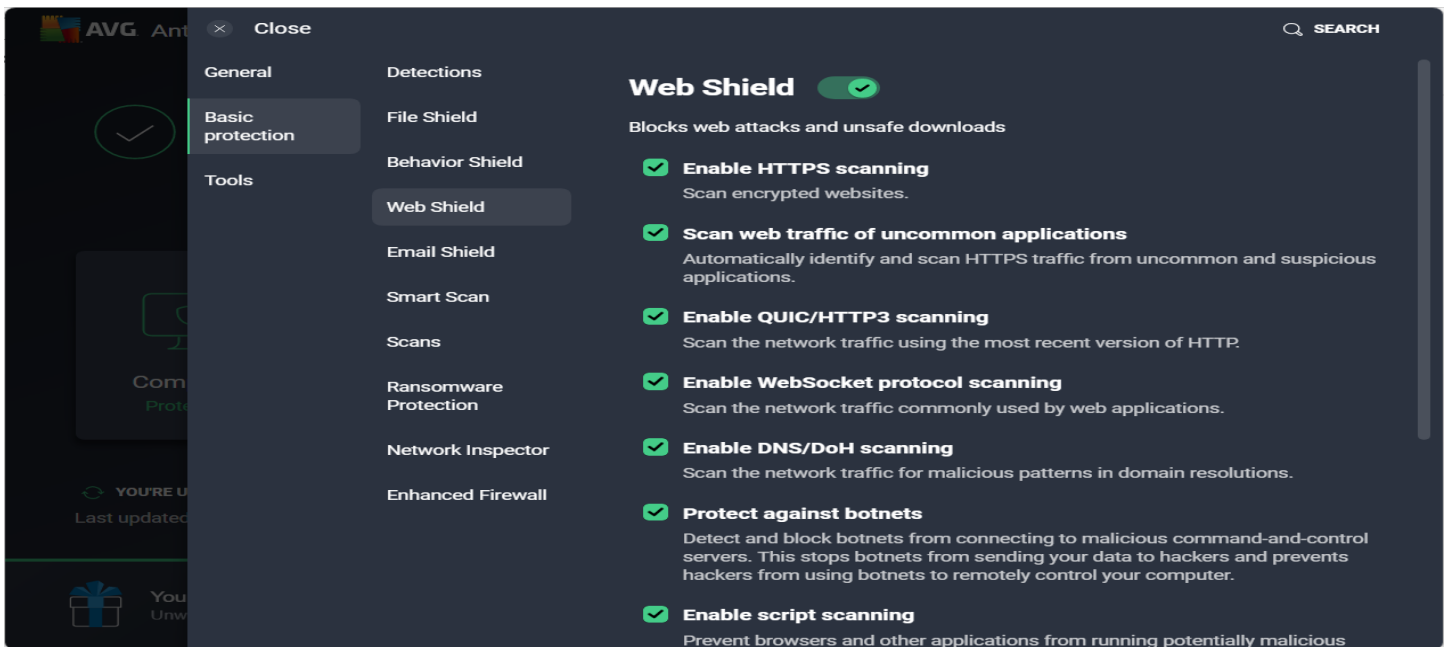
Application name	Status	Internet usage
Intel(R) System Usage Report	Active	853 MB
Fing Agent Service	Active	6 MB
Fing	Active	5 MB
Microsoft Edge	Active	5 MB
BasicService	Active	687 KB
Microsoft® Windows® Operating System	Active	427 KB
HiviewService	Active	51 KB
Microsoft Word	Active	44 KB
HwMdcCenter	Active	13 KB
HUAWEI PC Manager	Active	129 B



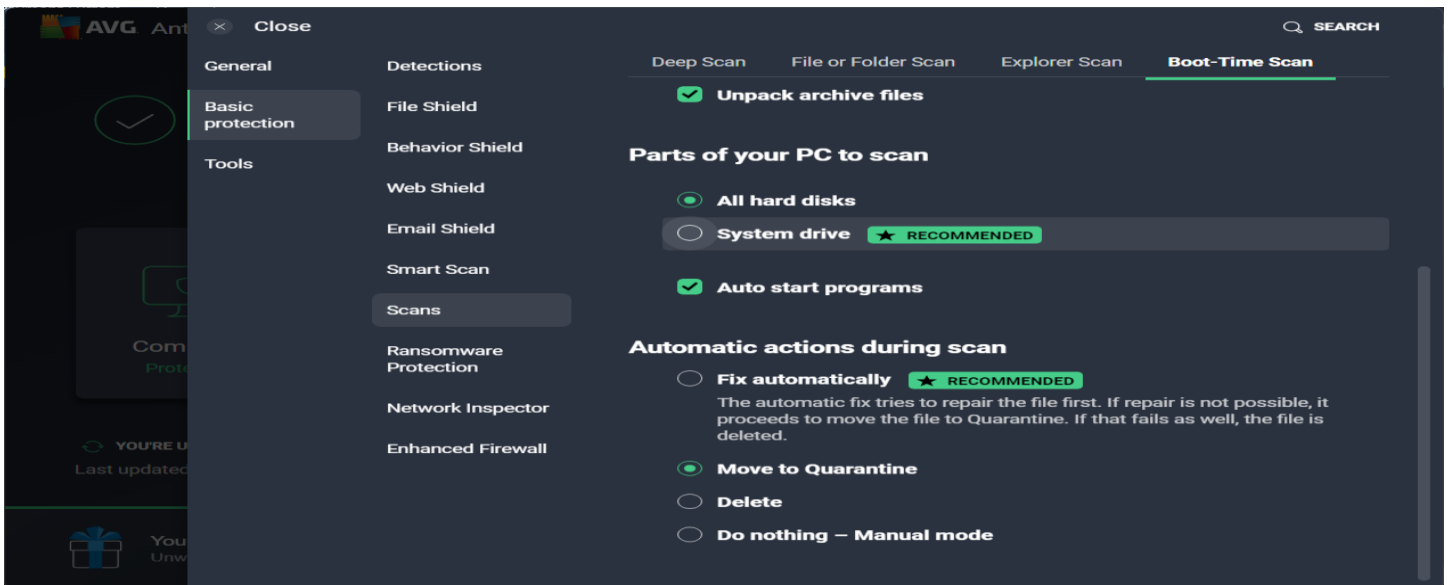
On this section I activated the Ransomware Protection in Brave, and NIUBI applications. In this it will prevent the software's from modifying my files for ransomware attacks. This is very important especially for NIUBI since it is used for partitioning my disk.



- To maximize the security, I set the Detection into High Sensitivity which is medium by default. I also checked the Enable Hardened Mode, since it is recommend for inexperienced users.



- On this I enabled HTTPS scanning and searched <https://secure.eicar.org/eicar.com>, to test effectiveness. This is the result of it, It will scanned the website and block the download before the page could prevent the virus.






















- In this section All hard disks om boot-time scan so that all my hard disk are scanned for vulnerabilities and threats every time I turn on my pc, strangely I expected that It would slow down the boot time of the laptop, but it didn't.














RULE LISTS: Here are the default rules set for the firewalls.

AVG AntiVirus Free									
Rule list									
BASIC RULES NETWORK RULES APPLICATION RULES									
These network rules will apply to any network you join, in the order below.									
Status / Name	Profile	Action	Protocol	Direction	Address	Local port	Remote port	ICMP Type	
Localhost Public	PUBLIC	ALLOW	TCP/UDP	IN/OUT	LOCALHOST				
DHCP Public	PUBLIC	ALLOW	UDP (17)	IN/OUT		67-68,546-547	67-68,546-547		
DNS Public	PUBLIC	ALLOW	TCP/UDP	OUT			53		
Windows Networking In Public	PUBLIC	BLOCK	TCP/UDP	IN		135-139,445			
Windows Networking Out Public	PUBLIC	ALLOW	TCP/UDP	OUT			135-139,445		
VPN - L2TP Public	PUBLIC	ALLOW	UDP (17)	OUT			1701		
VPN - L2TP ISAKMP Public	PUBLIC	ALLOW	UDP (17)	OUT		500	500		
VPN - L2TP IKE Public	PUBLIC	ALLOW	UDP (17)	OUT		4500	4500		
VPN - ESP Public	PUBLIC	ALLOW	ESP (50)	OUT					
VPN - AH Public	PUBLIC	ALLOW	AH (51)	OUT					
MS VPN - PPTP Public	PUBLIC	ALLOW	TCP (6)	OUT			1723		
GRE Public	PUBLIC	BLOCK	GRE (47)	IN/OUT					

BASIC RULES NETWORK RULES APPLICATION RULES

Status / Name	Profile	Action	Protocol	Direction	Address	Local port	Remote port	ICMP Type
  Icmp DestUnreachable	PRIVATE	ALLOW	ICMP (1)	IN/OUT				3  
  Icmp SourceQuench	PRIVATE	ALLOW	ICMP (1)	IN/OUT				4  
 VPN - L2TP	PRIVATE	ALLOW	UDP (17)	OUT			1701	
 VPN - L2TP ISAKMP	PRIVATE	ALLOW	UDP (17)	OUT		500	500	
 VPN - L2TP IKE	PRIVATE	ALLOW	UDP (17)	OUT		4500	4500	
 VPN - ESP	PRIVATE	ALLOW	ESP (50)	OUT				
 VPN - AH	PRIVATE	ALLOW	AH (51)	OUT				
 MS VPN - PPTP	PRIVATE	ALLOW	TCP (6)	OUT			1723	
 GRE	PRIVATE	ALLOW	GRE (47)	IN/OUT				
 Remote Desktop In	PRIVATE	ALLOW	TCP/UDP	IN		3389		
 PING OUT	PRIVATE	ALLOW	ICMP (1)	OUT				8
 PING_v6 OUT	PRIVATE	ALLOW	ICMPV6 (58)	OUT				128
 Traceroute OUT	PRIVATE	ALLOW	ICMP (1)	OUT				30

BASIC RULES NETWORK RULES APPLICATION RULES

Status / Name	Profile	Action	Protocol	Direction	Address	Local port	Remote port	ICMP Type
 Public Icmp Address In Block	PUBLIC	BLOCK	ICMP (1)	IN				17
 Public Icmp Trace Route In Block	PUBLIC	BLOCK	ICMP (1)	IN				30
 Public Icmp Domain Name In Block	PUBLIC	BLOCK	ICMP (1)	IN				37
 Public Icmp Destination Unreachable Out Block	PUBLIC	BLOCK	ICMP (1)	OUT				3
 Public Icmp Parameter Problem Out Block	PUBLIC	BLOCK	ICMP (1)	OUT				12
 Public Icmp6 Echo In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				128
 Public Icmp6 Listener Query In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				130
 Public Icmp6 Router Solicit In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				133
 Public Icmp6 Neighbor Solicit In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				135
 Public Icmp6 Information Query In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				139
 Public Icmp6 Inverse Neighbor Discovery Solicitation In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				141
 Public Icmp6 Certification Path Solicitation In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				148
 Public Icmp6 Multicast Router Solicitation In Block	PUBLIC	BLOCK	ICMPV6 (58)	IN				152