ESET Tech Center

IDS and advanced options in ESET Smart Security and ESET Endpoint Security

Ondersteuning | ESET Nederland - 2017-11-22 - Reacties (0) - Legacy

https://support.eset.com/kb2906

The IDS and advanced options section allows you to configure advanced filtering options to detect several types of attacks and vulnerabilities that can be carried out against your computer. **In some cases you will not receive a threat notification about blocked communications**. You can view the Personal firewall log to see all blocked incoming and outgoing communication attempts in the **Tools** › **Log files** section (from the **Log** drop-down menu select **Personal firewall**).

The availability of particular options in **Advanced setup** → **IDS and Advanced options** may vary depending on the type or version of your ESET product and Personal firewall module, as well as the version of your operating system.

To access IDS and advanced options in ESET Windows home products or ESET Endpoint Security, press the **F5** key on your keyboard, click **Firewall**, and then click **Edit** next to **IDS and advanced options**.

Figure 1-1

Click image to view larger in new window

Allowed services

Allow file and printer sharing in the Trusted zone – Allows remote computers in the Trusted zone to access your shared files and printers.
Allow UPNP for system services in the Trusted zone – Allows incoming and outgoing requests of UPnP protocols for

system services. UPnP (Universal Plug and Play also known as Microsoft Network Discovery) is used in Windows Vista and later operating systems.

Allow incoming RPC communication in the Trusted zone – Enables TCP connections from Trusted zone allowing access to MS RPC Portmapper and RPC/DCOM services.

Allow remote desktop in the Trusted zone – Enables connections via Microsoft Remote Desktop Protocol (RDP) and allows computers in Trusted zone to access your computer using a program that uses RDP (e.g. Remote Desktop Connection program).

Enable logging into multicast groups through IGMP – Allows incoming/outgoing IGMP and UDP multicast streams, for example video streams generated by applications using the IGMP protocol (Internet Group Management Protocol).

Maintain inactive TCP connections – In order to function, some applications require that the TCP connection that they establish is maintained even though the TCP connection may be inactive. Select this option to avoid terminating inactive TCP connections.

Allow communication for bridged connections – Select this option to avoid terminating bridged connections.

Allow response to ARP requests from outside the Trusted zone – Select this option if you want the system to respond to ARP requests with IP addresses that are not from Trusted zone. ARP (Address Resolution Protocol) is used by the network application to determine the Ethernet address.

Allow all traffic within the computer – If this option is disabled, you will be prompted to allow or deny localhost communication attempts. For this option to be operational the Personal firewall must be set to Interactive mode.

Allow Metro applications (Windows 8 only) – Communication of Windows Store applications that are running in the Metro environment is allowed according to Metro application manifest. This option will override all rules and exceptions for Metro applications regardless of whether you have selected Interactive mode or Policy-based mode in ESET personal firewall.

Alow incoming connection to admin shares in SMB protocol – The administrative shares (admin shares) are the default network shares that share hard drive partitions (C$, D$,

...) in the system together with the system folder (ADMIN$). Disabling connection to admin shares should mitigate many security risks. For example, the Conficker worm performs dictionary attacks in order to connect to admin shares.

Vista/Windows 7 services

Add IPv6 addresses from local network to the Trusted zone (fe80::/64) – Add a link-local address (IP address that is intended for communication in local network) from your local network that will be considered as a Trusted zone. Link-local addresses for IPv6 are assigned with the fe80::/64 prefix.
Allow automatic Web Services Discovery (WSD) for system services in the Trusted zone – Allows incoming or outgoing Web Services Discovery requests from Trusted zones thru the firewall. WSD is protocol used to locate services on a local network.
Allow multicast addresses resolution in the Trusted zone (LLMNR) – The LLMNR (Link-local Multicast Name Resolution) is a DNS packet based protocol that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link without requiring a DNS server or DNS client configuration. This option allows incoming/outgoing multicast DNS requests from/into the Trusted zone through the firewall.
Windows 7 HomeGroup support – Enables HomeGroup support for Windows 7 and later operating systems. A HomeGroup is able to share files and printers on a home network. To configure a Homegroup, navigate to Start > Control Panel > Network and Internet > HomeGroup.

Incoming RPC communication over SMB

MSRPC is the Microsoft implementation of the DCE RPC mechanism. Moreover, MSRPC can use named pipes carried into the SMB (network file sharing) protocol for transport (ncacn_np transport). MSRPC services provide interfaces for accessing and managing windows system remotely. Over the last years, several security vulnerabilities were discovered and exploited in the wild

in the Windows MSRPC system (Conficker worm, Sasser worm,...). Disable communication with MSRPC services that you do not need to provide to mitigate many security risks (such as remote code execution or service failure attacks).

Allow communication with the Security Account Manager service – This interface (samr) is used to communicate with the SAM (Security Account Manager) subsystem. SAM is a protected service that manages users and groups in Windows.
Allow communication with the Local Security Authority service – This interface (lsarpc) is used to communicate with the LSA (Local Security Authority) subsystem – a process in Windows (lsass.exe) that is responsible for enforcing the security policy of the system.
Allow communication with the Remote Registry service – This interface (winreg) is used to access to the registry, either locally or remotely. This enables remote users to modify registry settings on this computer.
Allow communication with the Service Control Manager service – This interface (svcctl) is used to manage Windows services via the SCM (Service Control Manager), which starts, stops and interacts with Windows service processes. Remote call to this service by an attacker can cause various problems.
Allow communication with the Server service – This interface (srvsvc) is used to manage the lanmanserver service (called Server service), that supports file, print, and named-pipe sharing over the network for this computer.
Allow communication with the other services – Allows communications with all other Microsoft RPC interfaces (such as Spooler service used for printers, or the Scheduler service).

Intrusion detection

CodeRed worm detection – Detects the CodeRed worm. CodeRed worm is a worm that uses a buffer overflow vulnerability to spread. The worm exploits a vulnerability in the indexing software distributed with IIS (Internet Information

Server).

ARP Poisoning attack detection – Detection of ARP poisoning attack caused by man in the middle attack or detection of sniffing at network switch. ARP (Address Resolution Protocol) is used by network application or device to determine the Ethernet address.

DNS Poisoning attack detection – Detection of DNS poisoning - recieving fake answer to DNS request (sent by attacker) which can point you to fake and malicious websites. DNS (Domain name systems) are distributed database systems that translate between human-friendly domain names and numeric IP addresses and allow users to refer to a website simply by using its domain name. Read more about this type of attack in the glossary.

TCP/UDP Port Scanning attack detection – Detects attacks of port scanning software - application designed to probe a host for open ports by sending client requests to a range of port addresses, with a goal of finding active ports and exploitoing vulnerability of the service. Read more about this type ofattack in the glossary.

Block unsafe address after attack detection – IP addresses that have been detected as sources of attacks are added to Blacklist to prevent connection for a certain period of time.

Display notification after attack detection – Turns on the system tray notification at the bottom right corner of the screen.

SqlSlammer worm detection – Detects attacks by the SqlSlammer worm. SqlSlammer worm causes a DoS on some Internet hosts and slows down general Internet traffic.

RPC/DCOM attack detection – If selected, attacks exploiting the Microsoft RPC DCOM vulnerability will be blocked.

Sasser worm detection – Detection of the Sasser worm. Another buffer overflow worm that affects computers running vulnerable versions of Windows XP/2000 and exploits the system through a port used by the Windows LSASS service.

SMB Relay attack detection – A type of attack where a remote party intercepts the communication between two computers. Read more about this type of attack in the glossary.

Conficker worm detection – Detection of the Conficker worm which targets the Windows OS using a Dictionary attack or Brute force on administrator's passwords.

Note: The aforementioned check boxes next to specific worm detection algorithms (such as Sasser) may not be available for all users. These features have been replaced by CVE detection in newer versions of ESET products or Personal firewall modules (see below).

Protocol SMB

Rogue server challenge attack authentication detection – This option protects you against an attack that uses a rogue challenge during authentication in order to obtain user credentials.
IDS evasion during named pipe opening detection – Detection of known evasion techniques used for opening MSRPCS named pipes in SMB protocol.
Detection CVE (Common Vulnerabilities and Exposures) – Implemented detection methods of various attacks, forms, security holes and exploits over SMB protocol. Please see the following CVE website at cve.mitre.org to search and obtain more detailed info about CVE identifiers (CVEs).

Protocol RDP – CVEs in RDP protocol (see above).

Protocol DCE/RPC – CVEs in the remote procedure call system developed for the Distributed Computing Environment (DCE).

Packet inspection

Deny old (unsupported) SMB dialects – Deny a SMB session with negotiated an old SMB dialect that are unsupported by IDS. Modern Windows operating systems support old SMB dialects due to backward compatibity with old operating systems such as Windows 95. The attacker can negotiate an old dialect in SMB session in order to evade traffic inspection. Deny old SMB dialects if your computer does not need to share files (SMB communication in general) with a computer with an old version of Windows.
Deny SMB sessions without extended security – Extended security can be negotiated during the SMB session negotiation in

order to provide more secure authentication mechanism than LAN Manager Challenge/Response (LM) authentication. The LM scheme is considered weak and not recommended for use.

Deny opening of executable files on a server outside the Trusted zone in SMB protocol – Drops connection when you are trying to open an executable file (.exe, .dll, ...) from a shared folder on the server that does not belong to the Trusted zone in Personal firewall. Note that copying executable files from trusted sources can be legitimate. On the other hand, this detection should mitigate risks from unwanted opening a file on a malicious server, for example caused by clicking a user on a link to a shared malicious executable file.

Deny NTLM authentication in SMB protocol for connecting a server in/outside the Trusted zone – Protocols that use NTLM (both versions) authentication schemes are subject to a credentials forwarding attack (known as SMB relay attack in case of SMB protocol). Denying NTLM authentication with a server outside the Trusted zone should mitigate risks from forwarding credentials by a malicious server outside the Trusted zone. Similarly, it can be denied NTLM authentication with servers in the Trused zone too.

Check TCP connection status – Checks to see if all TCP packets belong to an existing connection. If a packet does not exist in a connection, it will be dropped.

TCP protocol overload detection – The principle of this method involves exposing the computer/server to multiple requests – also see DoS (Denial of service attacks).

Verification of incoming/outgoing TCP and UDP packets (checksum validation) – Select this option for testing purposes only. This functionality validates the checksum of incoming/outgoing TCP/UDP packets.

ICMP protocol message checking – Prevents attacks that exploit the weaknesses of the ICMP protocol. Read more about this type of attack in the glossary.

Covert data in ICMP protocol detection – Checks to see if the ICMP protocol is used for data transfer. Many malicious techniques use the ICMP protocol to bypass the Personal firewall.

Troubleshooting

Log all blocked connections – Records all denied connections to a log.

Log blocked incoming worm attacks – Logs all attempts by worms to enter the system.
Enable advanced PCAP logging – Logs all network communication for troubleshooting purposes. A pop-up warning will notify user about the logging. Log files can be found in: *C:\ProgramData\ESET\ESET Smart Security\Diagnostics* on Vista and newer version of Windows or *C:\Documents and Settings\All Users\...* on older versions of Windows.

Tags
4.x
EES 6.x
ERA 6.x