ASECURITY

The Automatic SECURITY command provides many of the features of a custom-written security exit but without programming requirements.

Syntax:

```
ASECUrity [,ICMP={YES|NO}] [,FTPD={YES|NO}] [,FTPC={YES|NO}]
          [,ARP={YES|NO}] [,IPAV={YES|NO}] [,BLOCKIP={YES|NO}]
          [,BLOCKCNt=num]
```

Arguments

ICMP= - This parameter controls how the stack responds to PING requires.

YES - Allows normal responses to ICMP ECHO (ping) requests.

NO - Prevents VSE from responding to incoming ICMP PING requests. This is useful to stop "ping sweeps", commonly used to find active machines on a TCP/IP network. Note that this setting does not affect ping requests that originate on VSE.

FTPD= - This parameter controls how attempts to start an FTP session are handled.

YES - Allows normal connection to FTP Daemons.

NO - The “NO” option prevents new FTP sessions. Already-established sessions continue unaffected. Controls connection requests to the FTP Daemon. This can be used to temporarily stop new FTP sessions.

FTPC= - Similar to FTPD=, this parameter permits establishing an FTP connection but causes commands to be rejected with a “500 Command rejected” message.

YES - Commands are processed normally.

NO - The following commands are refused: USER, PASS, ACCT, QUIT, REIN, SYST, HELP, NOOP, PBSZ, PROT, and AUTH.

ARP= - This parameter controls the stack’s response to ARP requests.

YES - Allows normal ARP response.

NO - Requires SECURITY ARP=ON to already be in effect. Using this option prevents TCP/IP from responding to ARP requests. We are not sure why or when this would be useful.

IPAV= - This parameter controls all inbound IP traffic.

YES - Allows normal IP processing.

NO - Requires SECURITY IP=ON to already be in effect. Specifying "NO" will immediately prevent processing of all incoming IP datagrams. This is a drastic step, but one that might prove useful in the thick of an Internet attack.

BLOCKIP= - Allows automatic blocking of an IP address after it reaches a predetermined number of security violations. The ACCESS command can be used to reset the block for an IP address.

YES - Block access when the number of security violation attempts reaches the number specified by BLOCKCNT=.

NO - Do not automatically block access by IP address.

BLOCKCNt= - A numeric value between 1 through 255, inclusive. This is the number of security violation attempts that will be tolerated before an IP address is blocked from all access. This has meaning only when BLOCKIP=YES is in effect.

Example:

```
IPN237I asecurity icmp=yes,blockip=yes,blockcnt=10
IPN759I Security status change: Auto security changed ICMP=Y
IPN759I Security status change: Auto security changed BLOCKIP=Y
IPN473I Auto Security blocking by IP address Enabled
IPN474I Auto Security blocking by IP address after 10 violations
```

Notes:

- Use of the Automatic Security Exit is controlled by the SECURITY command. Once you have selected options with ASECURITY, you must still enable the exit with SECURITY.
- When blocking IP addresses, please remember that users may be behind a router that causes them to "share" a single IP address.
- If you use the Automatic Security feature, be sure that any user IDs (DEFINE USER) have the correct values in the DATA= field.

Related Commands:

ACCESS	-	Control access to VSE by IP address
DEFINE USER	-	Create a user ID and password.
DELETE USER	-	Remove a user ID and password entry.
ISOLATION	-	Prevents inbound connection requests from being honored.
PING_MESSAGE	-	Controls the "ping request received" console message.
QUERY ARPS	-	Displays the current content of the ARP table.
QUERY SECURITY	-	Displays current security settings.
QUERY USERS	-	Displays a list of defined user IDs.
SECURITY	-	Control TCP/IP security functions.