FTP/Armor™
Protect your Servers from FTP Attacks

How FTP/Armor works

FTP/Armor protects your servers from both Dictionary-based FTP Attacks and Brute Force FTP Attacks - regardless of server platform. The attack is detected and stopped before problems arise and the attacker is prevented from mounting another attack from the same place.

How FTP/Armor Works

To properly identify and stop an attack, FTP/Armor:

- Detects that an attack is happening
- Stops the current attack by killing the attackers connection
- Prevents future attacks by blocking further access to the FTP server from the offending IP address.
- Alerts IT staff of the attack and the actions taken.

Detecting the Attack

FTP/Armor monitors the FTP activity on all servers in the enterprise. It knows when an FTP client logon attempt fails.

Hacking attacks (especially Dictionary attacks) are characterized by the fact that they create a large number of failed logon attempts (usually for an unknown user ID or password) from a single IP address.

FTP/Armor keeps track of the number of logon failures by IP address. A threshold can be set to identify too many logon failures coming from a single IP address. When this threshold is reached, FTP/Armor will automatically classify the activity as an attack and react accordingly.

Stopping the Attack

FTP/Armor knows the IP address from which the attack is taking place. It issues a command to kill the connection in order to stop the current attack.

Preventing further Attacks

To prevent further attacks, FTP/Armor issues a command to block all activity from the attacking IP address, stopping the attack in its tracks and closing the exposure to your organization by preventing any further logon attempts from that FTP client.

You can choose to make this permanent or last only until the server is next restarted. As long as the traffic from the offending IP address is rerouted, new attacks from this IP address will be stopped before they even start.

On z/OS, FTP/Armor automatically submits a batch job to create a SAF security policy utilizing FTP/Guardian's SAF security interface for z/OS FTP. This JCL can be customized for use with RACF, ACF2 or TopSecret.

Alerting IT Staff about the Attack

Visibility is important when dealing with any kind of attacks. FTP/Armor will alert your organization that an attack was discovered and shut down by sending an alert email to any number of recipients.

The email informs your staff about a risk averted and the details of where the attack came from, when it started and when it was stopped.

On z/OS, FTP/Armor can additionally issue a console message (WTO), which can be a trigger for other automation tasks.

Phone: (678) 965 0885 • Email: sales@ftpsentry.com • Web: http://www.ftpsentry.com