DFL-M510 FAQ

FAQ

Q: Why does the device memory usage exceed 80% right after start-up?

Q: Why does D-Link strongly suggest not managing DFL-M510 from the Internet?

Q: Do the"Standby Hosts" disappear from the host table after rebooting?

Q: After rebooting the DFL-M510, what configuration files would disappear? (Host table? Policy? Report? …)

Q: What would happen after the hosts exceed 150 users?

Q: How does DFFL-M510 learn the host name? Why is the host name sometimes not shown? How often does it send the host name query?

Q: What LOG information is included in the DFL-M510?

Q: How many days of data is kept in the DFL-M510 for report?

Q: What would happen after the concurrent session exceeds 12K?

Q: What is the difference between Bypass Mode and Bypass feature (DMZ/Hosts)?

Q: How to implement the DFL-M510 in the environment with L3 device?

Q: On which occasions should I use the DMZ bypass or Host bypass? Why?

Q: How does the DFL-M510 manage internal hosts in the DHCP environment?

Q: How to deploy DFL-M510 in VLAN environment?

Q: Why is the login time so long? What factors affect this?

Q: How many groups/templates/user-defined patterns does the DFL-M510 support?

Q: What is the "Default Group" used for?

Q: Why is there Priority for each group in the DFL-M510?

Q: Are Hosts able to belong to multiple Groups at the same time?

Q: Why can the template only be applied to a pre-defined group? Why can it not be applied to a single host?

Q: Why is the "Wizard_Template" created by Setup Wizard unable to be modified?

Q: Why does the "Win Pop-up message" fail?

Q: Can the DFL-M510 send Pop-up messages to clients in different

Q: Why are there only 9 keyword filters in the DFL-M510?

Q: Why does RTM show no data?

Q: How many bytes are transferred from DFL-M510 to the PC for RTM?

Q: How often is the data refreshed in Real Time Application?

Q: What are the main features of RTM in DFL-M510?

Q: Is it possible to identify the victim infected malicious problem with RTM?

Q: How does H.323 work? By port? By protocol?

Q: How many P2P applications can the DFL-M510 manage?

Q: What's the difference between HTTP and web control in real-time application?

Q: Does Web Content keyword block ASCII code content? How does it work?

Q: What is the limitation to detect and block Skype?

Q: How does "Web Download" work? Are there any constraints?

Q: Does "Web Mail" pattern only detect the URL?

Q: Is there any detail Application list spported by the DFL-M510?

Q: How does DFL-M510 manage Streaming Media Applications?

Q: Why can the DFL-M510 only block or allow Skype / QQ? Is there no granular action control?

Q: How does DFL-M510 manage normal FTP and FTP applications like GETRight/FlashGet?

Q: Is the signature unidirectional or bidirectional?

MISC

Q: What happens after DFL-M510 blocks/detects malicious traffic?

Q: Is there any SNMP Set/Get/Trap list?

System

Q: Why does the device memory usage exceed 80% right after start-up?

A: To achieve robustness and efficiency, we do not allocate memory dynamically (runtime) in M510. Instead, we pre-allocate almost all necessary memory space for tables and data objects during booting up and then do the memory management by our own program, not the Operating System. Although the memory usage looks high right after the booting, it tends to keep stable (from 80% to 89%) without too much peaks.

Q: Why does D-Link strongly suggest not managing DFL-M510 from the Internet?

A: Since the communication between M-510 device and Java GUI could be quite bandwidth-consumptive (especially in signature download or firmware upgrade), the GUI communication possibly affects the upstream bandwidth and introduce more latency to outbound traffic. Moreover, the administrator may not have smooth RTM transaction by the way if the upstream bandwidth is quite limited.

Q: Do the"Standby Hosts" disappear from the host table after rebooting?

A: "Standby Hosts" will disappear only if device is reset to factory default status or the user manually removes them from UI. On the other hand, "Stand by Hosts" is stored in non-volatile memory so that rebooting the device does not clear it either. One noticeable technical issue is the M510 store the "Standby Hosts" temporarily in a one-way hash table, and a host record could be overwritten by another if hash collision happens.

Q: After rebooting the DFL-M510, what configuration files would disappear? (Host table? Policy? Report? …)

A: The report files and User Login logs will disappear after the reboot.

Q: What would happen after the hosts exceed 150 users?

A: Dropped or forwarded immediately. This is optional by setting the configuration "forward" or "block" flag in "Setup Host" page of UI.

Q: How does DFFL-M510 learn the host name? Why is the host name sometimes not shown? How often does it send the host name query?

A: DFL-M510 utilizes the WINS service to make queries for host names. Sometimes there is no name for a host in UI host table, and it may come from the following reasons:
It is not a Microsoft Windows platform and does not support the WINS services The host is enabled with the firewall embedded within Microsoft Windows platform and the firewall blocks the WINS service.
The WINS service is disabled by user
The host name query begins from the moment right after it has been learned by M-510, and the device negotiates with the host to get a name immediately. If the first query is failed, DFL-M51 0 will send the other two queries in a 5 minutes' interval. If these three queries all fail, the name learning process is closed for this host.

Q: What LOG information is included in the DFL-M510?

A: The DFL-M510 does not contain a disk to store large bulks of data for log and report, so therefore only the necessary information for network users is saved. Only "System Log" is saved at present.

Q: How many days of data is kept in the DFL-M510 for report?

A: DFL-M51 0 keeps 7-day reports in system memory but they will be gone if device is reset or reboot.

Q: What would happen after the concurrent session exceeds 12K?

A: Dropped or forwarded immediately. This is optional by setting the configuration "forward" or "block" flag in "Setup Host" page of UI.

Deployment

Q: What is the difference between Bypass Mode and Bypass feature (DMZ/Hosts)?

A: The Bypass Mode is performed by the system software, so that the packet information including protocol and throughput is still recorded by the device. On the other side, the Bypass feature is implemented by the hardware engine, so that although it's forwarding in wire-speed high performance, there will be no related information left.

Q: How to implement the DFL-M510 in the environment with L3 device?

A: We do not suggest a user to put any Layer 3 switch beneath the DFL-M510. Though it will not suffer the security and control management, the host information of traffic through the switch will be aggregated.

Q: On which occasions should I use the DMZ bypass or Host bypass? Why?

A: The DMZ is a trust area so that we do not have to check the traffic from this area and the high throughput is desired. The same idea is also applied for hosts. A network administrator can insert the DMZ servers into DMZ bypass list and host into host bypass list for the wire-speed performance from DFL-M510. (But there is no log/report for the bypassed traffic.)

Q: How does the DFL-M510 manage internal hosts in the DHCP environment?

A: The DFL-M510 identifies the internal hosts by their unique MAC addresses, so that the device will provide the precise traffic information and management capability in DHCP environments. When you enable the "MAC-Lock" feature in the host table, no matter how the IP address change, it would bind to the same MAC address.

Q: How to deploy DFL-M510 in VLAN environment?

A: In VLAN environment, the network administrator has to set up the supporting VLAN Group IDs (up to 8) through the DFL-M510 console or UI.

UI

Q: Why is the login time so long? What factors affect this?

A: In Login process, the Ul (by Java applet) reads several data and system configurations from the device and these suffer the login process. They include Network setting, DMZ list, Bypassed hosts, Host table, Schedule, Policy file, Operation Mode, Templates, Groups and Alert Message

Policy Setting

Q: How many groups/templates/user-defined patterns does the DFL-M510 support?

A: Group: 10 groups
Template: 20 templates (built-in templates included)
User-defined rule: 512 rules

Q: What is the "Default Group" used for?

A: All users belong to the Default group.

Q: Why is there Priority for each group in the DFL-M510?

A: If the host belongs to multiple groups, the policy will be different. For example, John belongs to Group A and Group B. The two group's policies are different. DFL-M510 differentiates based on group priority.

Q: Are Hosts able to belong to multiple Groups at the same time?

A: Yes, hosts can belong to multiple groups. But the policy will be different. The policy will depend on group priority.

Q: Why can the template only be applied to a pre-defined group? Why can it not be applied to a single host?

A: It is true that the user cannot apply the modified rule template to a single user. The user has to add the specified host into a host group before applying the rule template on it. We're doing this because we figured it's more convenient to divide Intranet hosts into different groups, and the administrator can define different templates accordingly. It makes more sense to operate on group level than host level because in general there are not many different templates in SME, and the policies applied to a host don't tend to change too often. Moreover, in our design a host can belong to different groups and

there're priorities among groups. For example, the CEO of the company can be in "Administrator" group and "Default" group in the same time. But he will only inherit the privilege of "Administrator" group due to its higher priority. But since there're priorities among host groups, we don't allow host-wise template operation because we cannot prioritize between the single host and a host group. Indeed it introduces a little inconvenience when applying a template to single host, but eventually the user benefits from the host group design

Q: Why is the "Wizard_Template" created by Setup Wizard unable to be modified?

A: This Template belongs to a pre-define template list, like the "Block all" Template. It cannot be modified/deleted. This Template is generated by System/Setup Wizard. If you want to modify it, please run *System/Setup* Wizard again.

Q: Why does the "Win Pop-up message" fail?

A: The Windows Pop-up messages are delivered through UDP packets and this service has low priority in Windows system. As the testing result shows, Windows system possibly could receive the WinPop-up messages without showing them up. Moreover, If the personal firewall is enabled in the system, the WinPop-up message could be blocked by the firewall policies. In addition, the WinPop-up service is able to be shutdown freely in the target system.

Q: Can the DFL-M510 send Pop-up messages to clients in different subnets under L3 switch?

A: WinPop-up messages are delivered by the DFL-M510 through UDP stream directly to the target (i.e., not through the gateway, even the target is in the different subnet). So that if the device and the target are not in the same subnet, the Win pop-up messages will not reach to the target host.

Q: Why are there only 9 keyword filters in the DFL-M510?

A: We believe that nine filters are enough for normal situations. Performance issue is another design consideration in this case.

Real-Time Monitor

Q: Why does RTM show no data?

A: The reasons may be:
1. Device is so busy that it couldn't send RTM to UI
2. There are some exceptions in UI's Java console
3. Device doesn't hit any rules (If no data means no top-n events)
Scenario 1 - the RTM shows no data while the time axis keeps going as time elapses: It may be because there is no network traffic passing through the device or the device is too busy to send the real-time data.
Scenario 2 - the time axis of the RTM does no go as time elapses: The RTM crashes because some unexpected error has happened. User may need to close the UI and re-login the system again.

Q: How many bytes are transferred from DFL-M510 to the PC for RTM?

A: The maximum is 120K bytes/5 sec. However, this only happens in extreme cases: 150 hosts fully learned, and 4096 rules hit in 5 seconds. The size of real-time information in clean traffic (i.e., no hit at all) is 104 bytes/5 sec.

Q: How often is the data refreshed in Real Time Application?

A: The data is refreshed every 5 seconds.

Q: What are the main features of RTM in DFL-M510?

A: Three main features of the real-time monitor:
1. The traffic monitor which allows administrator to monitor the traffic, in terms of bytes or bps, of selected types of applications.
2. The application monitor which allows the administrator to monitor the application usage of every managed host.
3. Two-layered Top N chart which allows the administrator to query from seven types of Top N list and or to further investigate another Top N list based on a selected result of the first Top N query. For example, the administrator has the possibility to query the Top N applications first and then query the Top N users of one of the selected result of the Top N applications.

Q: Is it possible to identify the victim infected malicious problem with RTM?

A: Yes. The victim information can be retrieved from the "Top 10 Health Concerns / Top 10 Users" and "Top 10 Users with Health Concern / Top 10 Health Concern" in DFL-M510 Real Time Monitor page of UI.

Application Pattern

Q: How does H.323 work? By port? By protocol?

A: We use a port range (TCP port 1023-5000) and specified patterns to identify the H.323 protocol, not only by single TCP port 1720.

Q: How many P2P applications can the DFL-M510 manage?

A: The applications for each P2P network are listed below:

Gnutella
BearShare *
Gnucleus *
Shareaza *
iMesh
KCeasy
Kiwi Alpha
For more information about P2P applications employing Gnutella network, please refer to below links:
http://en.wikipedia.org/wiki/Gnutella
http://www.slyck.com/gnutella. php?pacje=2

FastTrack
Kazaa *
Grokster *
MLDonkey *
iMesh
giFT-FastTrack
For more information about P2P applications employing FastTrack network, please refer to below Iinks:
http://www.slyck.com/ft.php?page=2
http://en.wikipedia.org/wiki/Fasttrack

eDonkey2000
eDonkey2000 *
eMule *
MLDonkey *
Shareaza *
Hydranode
MediaVAMP
Iphant
For more information about P2P applications employing eDonkey 2000 network,

please refer to below Iinks:
http://www.slyck.com/edonkey2k. php?page=2
http://en.wikipedia.org/wiki/EDonkey Network

BitTorrent
BitComet *
Azu reus
YetABC
WinMobile Torrent
For more information about P2P applications employing BitTorrent 2000 network, please refer to below links:
http://www.slyck.com/bt. php?page=2
http://en.wikipedia.org/wiki/Bittorrent

WinMX
WinMX *

DirectConnect
DirectConnect *
For more information about P2P applications employing DirectConnect network, please refer to below Iinks:
http:Ilwww.slyck.comldc. php?pacje=2

Ku ro
Kuro *
Pigo
Pigo *

Note: applications marked with * have been tested with DF-M510 device. Other applications listed above, though not officially tested with DFL_M51 0, should be blocked by M510 since they employ the P2P networks identified by DF-M510

Q: What's the difference between HTTP and web control in real-time application?

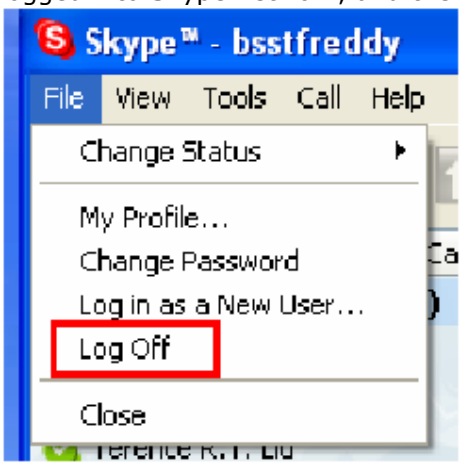
A: Web Control includes the categories of web application and web mail. HTTP is a subset of web control. For example, the action of Yahoo web mail is both in HTTP application and Web Control. However, the web mail utilization of Gmail is only classified into Web Control, because it follows HTTPS protocol.

Q: Does Web Content keyword block ASCII code content? How does it work?

A: It supports multiple encoding methods for different languages, and the Java applet will encode the input keyword according to the default encoding setting of the management console. If the input keyword string is not in ASCII characters, then it first will be encoded into a sequence of bytes using the default character set of the management client and saved to the device. The device will filter out the packets with the matching byte sequence. For example, if the user runs the management client on a PC and its default character set is Cpl 512 (Russian), and the user enters the keyword "решетчатая система". According to Cp1512, the given keyword will be encoded as the following byte sequence:
[OxFO, OxE5, OxF8, OxE5, OxF2, OxF7, OxEO, OxF2, OxEO, OxFF, 0x20, OxFl, OxE8, OxFl, OxF2, OxE5, OxEc, OxEO]
Packets with a matching byte sequence will be filtered out as they are received by the device. However, the same string encoded in a different way will pass through the device provided no other filter catches it.

Q: What is the limitation to detect and block Skype?

A: With DFL-M510-Pattern-3.16, there are two known constraints for blocking Skype:
1. A network administrator sets DF-M510 to block Skype ***after*** an internal user has logged into Skype network, and the user never logs off.



2: A user first logs in to Skype network with his/her computer at one place, does not log off, and then connects his/her computer to the network managed by DFL-M510.

Note: by definition, the behaviour below is called **quit** Skype network, which is different from the behaviour of **log off** Skype.

Q: How does “Web Download” work? Are there any constraints?

A: The “Web download’ in DF-M510 stands for a network behaviour that employs HTTP GET command to download files from a web server. When a user clicks a download link and tries to download files, the browser sends an HTTP GET request to the web server. At the same time the file name to be downloaded and the file location are also sent with the HTTP GET request. By identifying HTTP GET request and the file extension name, which usually identifies the file format of the file, DF-M510 is able to know that a user is trying to download a file.

Below is a list of common file types and their file extension names. File extension name supported by “Web download” is marked with YES in the last column.

AP class	AP name	Extension	Content-Type	Support
Office	MS Word	doc	application/msword	Yes
	MS Powerpoint	ppt	application/vnd.ms-powerpoint	Yes
	MS Excel	xls	application/vnd.ms-excel	Yes
	Adobe acrobat	pdf	application/pdf	Yes
	Notepad	txt	text/plain	
	Text RTF	rtf	application/rtf	
Compression	ZIP	zip	application/zip	Yes
	RAR	rar		Yes
	TAR	tar	application/x-tar	Yes
	GZ	gz	application/x-gzip	Yes
	BZ2	bz2	application/x-bzip2	Yes
	Redhat RPM	rpm	application/x-redhat-package-manager	Yes
Excutable file	Windows	exe	application/octet-stream	Yes
Audio	AAC	M4p		
	MP3	mp3		
Video	Mpeg2	mpg		
Graph	PNG	png		
	GIF	gif	application/gif	
	JPG	jpg	application/jpeg	
	TIFF	tiff	application/tiff	

Q: Does "Web Mail" pattern only detect the URL?

A: No. As for Yahoo web mail, DFL-M510 identifies the behaviour of opening web mail pages after a user has logged in to Yahoo web mail. As for Hotmail, DFL-M510 blocks URL plus parameters that are necessary for web mail services. For Gmail, DFL-M510 block URLs that are known to connect to Gmail.

Q: Is there any detail Application list spported by the DFL-M510?

A: Yes. Please refer to the ***DFL-M510 Application Pattern List*** provided by D-Link.

Q: How does DFL-M510 manage Streaming Media Applications?

A: DFL-M510 manages Streaming Media Applications by identifying signatures of Streaming Media Applications.

Q: Why can the DFL-M510 only block or allow Skype / QQ? Is there no granular action control?

A: After a user logs into Skype or QQ, all the transmission is encrypted and as a result there is no significant signatures of their other behaviours such as sending messages, sending files, or voice chatting.

Q: How does DFL-M510 manage normal FTP and FTP applications like GETRight/FlashGet?

A: Because GetRight/FlashGet is management software of downloading files, when users use GetRightlFlashGet to download files via FTP, such network behaviour acts like a normal FTP application and makes no difference between normal FTP and other FTP management applications. As such, DFL-M510 can not distinguish between normal FTP and other FTP management applications.

Q: Is the signature unidirectional or bidirectional?

A: The direction of the signature varies from one application to another. It's all up to the behaviour.
For signatures detecting IM's behaviours such as File Transfer, Chat, Online Game, Audio Communication, and Video Communication, the directions are bidirectional. This means that DFL-M510 can detect such attempts either from LAN to WAN or from WAN to LAN.
For signatures detecting HTTP download attempts, IM login attempts, Web Mail controls (Yahoo Mail, Gmail, and Hotmail), Web Upload, Web Download, and Java Applet download attempts, the directions are unidirectional.
For signatures detecting malicious traffic made by worm/Trojan, the direction is bidirectional.

MISC

A: Worm/Trojan List

Item	Description
1	WORM Windows Lsasrv.dII RPC Overflow(Sasser)
2	WORM Windows Lsasrv.dII RPC Overflow (Sasser)-1
3	WORM Windows Lsasrv.dII RPC Overflow Unicode (Sasser)
4	WORM Windows Lsasrv.dII RPC Overflow Unicode (Sasser)-1
5	WORM HTTP IIS CodeRed
6	WORM IIS default.ida access (CodeRed v2)
7	WORM DCOM System Shell Expicit Response (Blaster)
8	WORM DCOM Successful Shell Exploit Response (Blaster)
9	WORM Windows RPC DCOM Interface exploit - 135 (Blaster)
10	WORM Windows RPC DCOM Interface exploit - 445 (Blaster)
11	WORM Windows RPC DCOM Bind attempt (Blaster)
12	WORM WEB-IIS WebDAV exploit attempt.a (Blaster)
13	MISC OpenSSL Worm traffic
14	WORM slapper admin traffic
15	DoS MS-SQL Slammer Worm
16	WORM .emf Heap Overflow (M504-032) -1
17	WORM .emf Heap Overflow (M504-032) -2
18	WORM .emf Heap Overflow (M504-032) -3
19	WORM M504-034 zipped Folders Exploit via http
20	WORM M504-034 zipped Folders Exploit via smtp_1
21	WORM M504-034 zipped Folders Exploit via smtp_2
22	WORM M504-034 zipped Folders Exploit via smtp_3
23	WORM RealPlayer SMIL File Handling Buffer Overflow

B. Trojan/Backdoor

Item	Description
1	TROJAN LSASS.EXE 53/TCP
2	BACKDOOR Malice over SMTP
3	BACKDOOR Malice IRC serier ping
4	BACKDOOR Malice IRC serier message
5	ACKcmdC trojan scan
6	QAZ Worm Client Login access
7	CDK
8	shaft agent to handler
9	FINGER cmd_rootsh backdoor attempt
10	BACKDOOR hack-a-tack attempt
11	MISC ramen worm outgoing
12	WEB-MISC OpenSSL Worm/Slapper
13	linux rootkitftp attempt (IrkrOx)
14	linux rootkitftp attempt (dl3hh[)
15	linux rootkit ftp attempt (satori)
16	linux rootkit ftp attempt (haxOr)
17	BACKDOOR Remote PC Access connection attempt
18	TROJAN active-BackOrifice 1 -web
19	TROJAN active-BackConstruction 2.1 ftp open reply
20	TROJAN dagger_1 .4.0_client_connect
21	TROJAN active-netbus-12346
22	TROJAN worm-QAZ calling home
23	TROJAN BackOrificel-scan
24	TROJAN trojan-hOrtiga
25	TROJAN active-netbus-12345
26	TROJAN active-DeepThroat
27	TROJAN active-BackConstruction 2.1 ftp open reques
28	TROJAN active-HackAttack 1.20
29	TROJAN active-mosuckeri 1-badlogin
30	TROJAN active-DoIy2.0
31	TROJAN active-PhaseZero serier
32	TROJAN active-Infector 1.6 serier to client
33	TROJAN active-deepthroat_ftpd
34	TROJAN active-CAFEiniO.9
35	TROJAN netbus-getinfo-12346
36	TROJAN active-DonaidDick 1.53
37	TROJAN worm-QAZ infection
38	TROJAN active-subseven22
39	TROJAN active-mosucker2l
40	TROJAN active-BackConstruction 2.1
41	TROJAN ative-SatansBackdoor.2.0.Beta
42	TROJAN active-BackOrifice 1 -d jr
43	TROJAN active-dagger_1 .4.0

44	TROJAN Y3K-Rat-1 .3
45	TROJAN netbus-getinfo-12345
46	TROJAN active-BackOrificel-info
47	BACKDOOR FsSniffer connection attempt
48	BACKDOOR DoomJuice file upload attempt
49	TROJAN apple.net query
50	Trojan Netbus 2.1
51	BACKDOOR SubSeven 2.0 server connection response
52	Trojan BackOrifice 2000 ver 1.0 server connection response
53	Trojan BackOrifice 2000 ver 1.1 serier connection response -1
54	Trojan Evilbot connecting IRC server
55	TROJAN Slackbot active
56	TROJAN Phel.A infecting attempt
57	TROJAN Ceegar infecting attempt
58	BACKDOOR DeepThroat 3.1 Server Response - 3150

Q: What happens after DFL-M510 blocks/detects malicious traffic?

A: By Layer 7 detection engine, DFL-M510 will drop the corresponding packet which is classified as a malicious packet. Furthermore, the device logs the event for the report and sends the data to the real-time monitor of UI if it exists. If this malicious behaviour is through TCP connection, then the connection will be blocked and put into a black list for denying further communication.

Q: Is there any SNMP Set/Get/Trap list?

A: The user can set the following SNMP objects: sysName, sysContact, and sysLocation. The user can get the following SNMP objects: sysName, sysContact, sysLocation, and sysDescr.
The device sends the SNMP trap messages when system boot up and the change of link status (link up/down).