How to setup Anti-Virus Scanning

This example shows how to setup an Anti-Virus scanning policy for HTTP traffic from "LAN" to "all-nets". We will assume there is already a NAT rule defined in the IP rule set to NAT this traffic.



(1) Create an HTTP ALG Object "HTTP-ALG-AV".

(2) Select "Protect" in the "Mode" dropdown list.



(3) Then, create a "Service object" using the new "HTTP AFG".

D-Link Building Networks for People	®					2	Logged in as administrator admin - 192.168.1.100	
😚 Home 🛛 📉 Configuration 🗸 🗌	Tools 🚽	🕤 Status 🗸	Naintenance 🗸				😚 Logout	👔 неір
DFL-260 G System Objecte Dobjecte	ŕ	Services Services are pre-d	defined or user-defined objects representing vari	ious IP protocols, such a	s HTTP, FTP and Telnet.			
ALG with AV/WCF		# 🖝	Name	Type	Darametere	ALC Info	Comments -	
Services		1	TCP-services	ТСР	80,443	HTTP-ALG-AV - AV:Protect		
- 1 Pools		2	😥 l2tp-raw	Group	l2tp-ctl, l2tp-encap		L2TP control and transport, unencrypted	
		3	😥 ipsec-esp	IPProto	50		IPsec ESP (encrypted and authenticated)	
	E	4	🔯 ipsec-ah	IPProto	51		IPsec AH (authenticated	
E NPN Objects		5	🧑 ipsec-natt	UDP	4500		IPsec NAT-traversal (through udp/4500)	
HTTP Banner Files		6	😥 ipsec-suite	Group	ipsec-natt, ipsec-ah, ipsec- esp, ike		The IPsec+IKE suite	
E- \$ IP Rules		7	🐼 http-outbound-wcf	тср	80	http-outbound-wcf - WCF:Enabled	HTTP via HTTP ALG "http- outbound-wcf". Web Content	
lan_to_wan		8	🙀 http-outbound-av	TCP	80	http-outbound-av - AV:Protect	HTTP via HTTP ALG "http- outbound-av", Antivirus en	
Access		9	🙀 http-outbound-av-wcf	TCP	80	http-outbound-av-wcf - AV:Protect, WCF:Enabled	HTTP via HTTP ALG "http- outbound-av-wcf". Antiviru	
- 😽 Ethernet		10	🔯 ftp-outbound-av	TCP	21	ftp-outbound-av - AV:Protect	FTP - protects client against data channel attacks	
WUAN		11	😥 ftp-passthrough-av	TCP	21	ftp-passthrough-av - AV:Protect	FTP - unrestricted - allows all transfer modes for	
		12	🙀 smtp-inbound	TCP	25	smtp-inbound	Simple Mail Transfer Protocol via SMTP ALG.	
PPPoE		13	🐼 smtp-inbound-av	тср	25	smtp-inbound-av - AV:Protect	Simple Mail Transfer Protocol via SMTP ALG. Antivi	
		14	🔯 all_services	IPProto	0-255		All possible IP protocols	

(4) Select the "TCP" in the "Type" dropdown list. Enter 80 and 443 in

the "Destination Port" textbox. Select the "HTTP-ALG-AV" just created in the ALG dropdown list.

D-Link Building Networks for People	2 :	Logged in as administrator admin - 192.168.1.100
😚 Home 📉 Configuration 🗸 🎢 Tools	; 🗸 🛛 😋 Status 🗸 🛛 🗞 Maintenance 🗸	😚 Logout 🔰 👔 Help
DFL-260 DFL-260 Dipets Dipe	CP-Services A TCPUDP Service is a definition of an TCP or UDP protocol with specific parameters General Ceneral Ceneral	
Sentces S	Name: TCP-services Type: TCP Source: 0-65535 Destination: 80.443 Image: Topologic and the port ranges separated by commas. For example: 137-138,445 Image: Pass returned ICMP and messages from destination Image: Topologic and the port of the part of	
Control Contr	SYN thood protection (SYN Relay) Application Layer Gateway An Application Layer Gateway (XLO; capable of managing advanced protocol; can be specified for this service. A.G. INTTP-ALG-AV V Max Bession: 200 Specifies how many concurrent sessions that are permitted using this service. Comments Comments	

(5) Create a new IP Rule. Select the new service, "TCP-services", in the

"Service" dropdown list. Anti-Virus scanning is now activated for

D-Link Building Networks for People	® Le							Sector Log	ged in as administrator in - 192.168.1.100	
😚 Home 🛛 📉 Configuration 🗸 🗌	🏋 Tools 🚽	🕤 Status 🗸	Naintenance	-					😚 Logout 📔 👔 Help	р
DFL-260 B OSystem Dijects	-	B IP Rules	to filter IP-based network tra	iffic. In addition, they pro	wide means for address trans	slation as well as Server Load	Balancing.			
Address Book ALG with AV/WCF Services IP Pools MAT Reals		# • 1 2	Name	Action	Src If	Src Net	Dest If	Dest Net	Service CP-services	
Authentication Objects VPN Objects HTTP Banner Files	Е	5	18 101/20_4011					(j) Right-	dick on a row for additional options.	
Rules SilP R										
C C C C C C C C C C C C C C C C C C C										

all web traffic from "lannet" to "all-nets".

D-Link Building Networks for People		Logged in as administrator admin - 192 168 0.10
😙 Home 📉 Configuration 🗸 🎢 To	ools 🗸 🛛 😋 Status 🗸 🛛 🔩 Maintenance 🗸	😚 Logout 🕴 👔 Help
DFL-260 DFL-260 DFL-260 DOsete Address Book DAG with AV/WCF Schedules Pools NAT Pools Dosete Authentication Construction Dosete Dosetee Doseteee Doseteeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	EntreParent An Prole specifies what action to perform on network traffic that matches the specifies filter ortents. General Log Settings NAT SAT Multiplex SAT Ceneral Bester if logging should be enabled and what severity to use Demole logging Log with severity: Alert	OK Cancel

D-Link Building Networks for People								실 Logg admi	ed in as administrator n - 192.168.1.100	
😙 Home 🛛 📉 Configuration 🗸 🛛 🎢 Too	ls 🗸 📔 🛐 Status 🗸	🛛 Nainte	nance 🗸						😚 Logout	👔 Help
DFL-260	Anti-Vin	us Log								
E Cystem	Anti-Virus L	Da								
Address Book	Each search field uses	strict matching pol	licy. Wildcard searches are don	e by using ** to mat	ch zero or more arbitrary ch	aracters '?' matches one a	whitrary character			
ALG with AV/WCF Services Services War Pools Services War Pools Services War Pools Services War Pools Services Services Services Services Services Services	Time: Source Interface: IP Address: Port: Event: Severity: Free Text: Internal Logging (1-2:	2)	To Destination Action: Cetegory: (Any) Sear	th Reset					Refresh Log 🖉 Clear I	99
- Khernet	Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action	
	2011-02-21 06:07:24	Warning	ANTIVIRUS 5800001		тср	lan core	192.168.1.100 188.40.238.250	49893 80	virus_found block_data	
	filename="eicar.o	om" virusname	="EICAR-Test-File" viruss	ig="EICAR-Test	-File" advisoryid="AV1	algmod=http algses	ad=42 origsent=1378 t	ermsent=620 A	visory link	
PPPoE	06:07:14 filename="eicar_	Warning com.zip* virusna	5800001 ame="EICAR-Test-File" vi	russig="EICAR-	TCP Test-File" advisoryid="	core AV1" algmod=http alg	188.40.238.250 gsesid=41 origsent=71	80 .7 termsent=84	block_data Advisory link	

Anti-Virus scanning is now activated for all web traffic from "lannet" to "all-nets".