

How To Einstellen Logging für Firewallregeln

[Voraussetzungen]

1. DSR-500N/1000N mit Firmware Version: v1.06B43 und höher

[Szenario]

PC1-(192.168.10.100/24)-{LAN}-[DSR-500N]-(1.1.1.1/24)-{WAN}---PC2 (1.1.1.100/24)

[Schritte]

1. Einrichten einer Firewall-Regel (Service HTTP) und Weiterleiten zum PC1
2. Aktivieren der Option Log "Always" innerhalb der gerade erstellten Firewall-Regel

FIREWALL RULES											LOGOUT
A firewall is a security mechanism to selectively block or allow certain types of traffic in accordance with rules specified by network administrators. You can use this page to manage the firewall rules that control traffic to and from your network. The List of Available Firewall Rules table includes all firewall rules for this device and allows several operations on the firewall rules.											
List of Available Firewall Rules											
<input type="checkbox"/>	#	Status	From Zone	To Zone	Service	Action	Source Hosts	Dest Hosts	Local Server	Internet Dest	Log
<input type="checkbox"/>	1	Enabled	WAN	LAN	HTTP	Allow Always	Any		192.168.10.100	WAN1	Always

3. gehen Sie zu “Tools > Log Settings > Log Facility” und aktivieren Sie alle Logeinträge bei den Optionen “System” & “Kernel”

LOGS FACILITY LOGOUT

This page allows user to set the date and time for the router. User can use the automatic or manual date and settings depending upon his choice.

Logs Facility

Facility: System

Display and Send Logs

	Display in Event Log	Send to Syslog
Emergency:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alert:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Critical:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Error:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Warning:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Notification:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Information:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Debugging:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

LOGS FACILITY LOGOUT

This page allows user to set the date and time for the router. User can use the automatic or manual date and settings depending upon his choice.

Logs Facility

Facility: Kernel

Display and Send Logs

	Display in Event Log	Send to Syslog
Emergency:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Alert:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Critical:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Error:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Warning:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Notification:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Information:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Debugging:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. gehen Sie zu “Tools > Log Settings > Logs Configuration“ und aktivieren Sie die Option “WAN to LAN”

LOGS CONFIGURATION
LOGOUT

This page allows user to configure system wide log settings.

Routing Logs

	Accepted Packets	Dropped Packets
LAN to WAN:	<input type="checkbox"/>	<input type="checkbox"/>
WAN to LAN:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>
DMZ to WAN:	<input type="checkbox"/>	<input type="checkbox"/>
LAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>
DMZ to LAN:	<input type="checkbox"/>	<input type="checkbox"/>
VLAN to VLAN:	<input type="checkbox"/>	<input type="checkbox"/>

System Logs

All Unicast Traffic:	<input type="checkbox"/>
All Broadcast / Multicast Traffic:	<input type="checkbox"/>
FTP Logs:	<input type="checkbox"/>
Redirected ICMP Packets:	<input type="checkbox"/>
Invalid Packets:	<input type="checkbox"/>

Other Events Logs

Bandwidth Limit:	<input type="checkbox"/>
------------------	--------------------------

5. wenn PC2 auf die IP 1.1.1.1 im Browser zugreift können Sie im Log unter „Status > Logs > View All Logs“ die entsprechenden Einträge sehen

```
Thu Sep 13 11:10:48 2012 (GMT) [DSR-500N][kernel][KERNEL] WAN_LAN[ACCEPT] IN=WAN OUT=LAN SRC=1.1.1.100 DST=192.168.10.100 PROTO=TCP SPT=55344 DPT=80
Thu Sep 13 11:10:48 2012 (GMT) [DSR-500N][kernel][KERNEL] WAN_LAN[ACCEPT] IN=WAN OUT=LAN SRC=1.1.1.100 DST=192.168.10.100 PROTO=TCP SPT=55343 DPT=80
```