

Langsame oder keine Namensauflösung bei Benutzung der DSR-Serie (250N/500N/1000N) als Gateway

Szenario:

In einem Netzwerk wird ein Gerät der DSR-Serie als Internetgateway betrieben. Unter bestimmten Umständen (z.B. größere Anzahl Clients) kann die Namensauflösung durch die Angriffsprüfung als Angriff gewertet und somit blockiert werden.

Lösung

- 1.) Verbinden Sie sich auf den DSR
 - a. Wechseln Sie in das Menü „Advanced -> Advanced Network -> Attack Checks“

The screenshot shows the D-Link web interface for a DSR-1000N router. The top navigation bar includes 'DSR-1000N', 'SETUP', 'ADVANCED' (circled in red), 'TOOLS', 'STATUS', and 'HELP'. The left sidebar menu has 'Advanced Network...' (circled in red) selected, with a sub-menu showing 'Attack Checks' (circled in red). The main content area displays 'APPLICATION RULES' and a table titled 'List of Available Application Rules' with columns for Protocol, Interface, Outgoing Ports, and Incoming Ports. A 'Helpful Hints...' sidebar on the right provides additional information.

Protocol	Interface	Outgoing Ports		Incoming Ports	
		Start Port	End Port	Start Port	End Port

b. deaktivieren Sie die Option "Block UDP flood"

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.06B99_VW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules Website Filter Firewall Setting... Wireless Settings Advanced Network... Routing Certificates External Authentica Users IP/MAC Binding IPv6 Captive Portal Switch Settings Intel® AMT Package Manager

ATTACK CHECKS LOGOUT

This page allows you to specify whether or not to protect against common attacks from the LAN and WAN networks.

Save Settings Don't Save Settings

WAN Security Checks

Enable Stealth Mode:
Block TCP flood:

LAN Security Checks

Block UDP flood:
UDP Connection Limit: 25
Allow Ping from Lan:

ICSA Settings

Block ICMP Notification:
Block Fragmented Packets:
Block Multicast Packets:
Block Spoofed IP Packets:

DoS Attacks

SYN Flood Detect Rate [max/sec]: 128
Echo Storm [ping pkts./sec]: 15
ICMP Flood [ICMP pkts./sec]: 100

Helpful Hints... For added security, it is recommended that you enable Stealth Mode. This blocks ping and ARP response from the WAN interfaces. Ping is often used by malicious Internet users to locate active networks or PCs. More...

UNIFIED SERVICES ROUTER

Anschließend prüfen Sie bitte erneut das Verhalten z.B. mittels eines „nslookup“