DCFW-1800 Series Next Generation Firewalls

N9040

N8420

N7210

N6008

N5005

N3002

N2002

Product Overview

The DCN Next Generation Firewall (NGFW) provides comprehensive and granular visibility and control of applications. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications. The DCN NGFW incorporates comprehensive network security and advanced firewall features, provides superior price

performance, excellent energy efficiency, and comprehensive threat prevention capability.

Product Highlights

Granular Application Identification and

The DCFW-1800 NGFW provides fine-grained control of web applications regardless of port, protocol, or evasive action. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. Security Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking unauthorized or malicious applications.

Control Comprehensive Threat Detection and Prevention

The DCFW-1800 NGFW provides real-time protection for applications from network attacks including viruses, spyware, worms, botnets, ARP spoofing, DoS/DDoS, Trojans, buffer overflows, and SQL injections. It incorporates a unified threat detection engine that shares packet details with multiple security engines (AD, IPS, URL filtering, Anti-Virus, Sandbox etc.), which significantly enhances the protection efficiency and reduces network latency.

Features

Network Services

• Dynamic routing (OSPF, BGP, RIPv2)
• Static and Policy routing
• Route controlled by application
• Built-in DHCP, NTP, DNS Server and DNS proxy
• Tap mode – connects to SPAN port
• Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking)
• L2/L3 switching & routing
• Virtual wire (Layer 1) transparent inline deployment

Firewall

• Operating modes: NAT/route, transparent (bridge), and mixed mode
• Policy objects: predefined, custom, and object grouping
• Security policy based on application, role and geo-location
• Application Level Gateways and session support: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
• NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
• NAT configuration: per policy and central NAT table
• VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
• Global policy management view
• Security policy redundancy inspection

• Schedules: one-time and recurring

Intrusion Prevention

• Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
• IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
• Packet logging option
• Filter Based Selection: severity, target, OS, application or protocol
• IP exemption from specific IPS signatures
• IDS sniffer mode
• IPv4 and IPv6 rate based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)
• Active bypass with bypass interfaces
• Predefined prevention configuration

Anti-Virus

• Manual, automatic push or pull signature updates
• Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP
• Compressed file virus scanning

Attack Defense

• Abnormal protocol attack defense
• Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
• ARP attack defense

URL Filtering

• Flow-based web filtering inspection
• Manually defined web filtering based on URL, web content and MIME header
• Dynamic web filtering with cloud-based real-time categorization database: over 140 million URLs with 64 categories (8 of which are security related)
• Additional web filtering features:
- Filter Java Applet, ActiveX or cookie
- Block HTTP Post
- Log search keywords
- Exempt scanning encrypted connections on certain categories for privacy
• Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP
• Web filter local categories and category rating override

Cloud-Sandbox

• Upload malicious files to cloud sandbox for analysis
• Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP and FTP
• Support file types including PE,ZIP, RAR, Office, PDF, APK, JAR and SWF
• File transfer direction and file size control
• Provide complete behavior analysis report for malicious files

IP Reputation

• Botnet server IP blocking with global IP reputation database

SSL Decryption

• Application identification for SSL encrypted traffic
• IPS enablement for SSL encrypted traffic
• AV enablement for SSL encrypted traffic
• URL filter for SSL encrypted traffic
• SSL Encrypted traffic whitelist
• SSL proxy offload mode

Endpoint Identification

• Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
• Support 10 operation systems
• Support query based on IP and endpoint quantity

File Transfer Control

• File transfer control based on file name, type and size
• File protocol identification, including HTTP, HTTPS, FTP, SMTP, POP3 and SMB protocols
• File signature and suffix identification for over 100 file types

Application Control

• Over 3,000 applications that can be filtered by name, category, subcategory, technology and risk
• Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
• Actions: block, reset session, monitor, traffic shaping
• Identify and control cloud applications in the cloud
• Provide multi-dimensional monitoring and statistics for cloud applications, including risk category and characteristics

Quality of Service (QoS)

• Max/guaranteed bandwidth tunnels or IP/user basis
• Tunnel allocation based on security domain, interface, address, user/user group, server/server group, application/app group, TOS, VLAN
• Bandwidth allocated by time, priority, or equal bandwidth sharing
• Type of Service (TOS) and Differentiated Services (DiffServ) support
• Prioritized allocation of remaining bandwidth
• Maximum concurrent connections per IP

Server Load balancing

• Weighted hashing, weighted least-connection, and weighted round-robin
• Session protection, session persistence and session status monitoring
• Server health check, session monitoring and session protection

Link Load balancing

• Bi-directional link load balancing
• Outbound link load balancing includes policy based routing, ECMP and weighted, embedded ISP routing and dynamic detection
• Inbound link load balancing supports Smart DNS and dynamic detection
• Automatic link switching based on bandwidth, latency, jitter, connectivity, application etc.
• Link health inspection with ARP, PING, and DNS

VPN

• IPSec VPN
- IPSEC Phase 1 mode: aggressive and main ID protection mode
- Peer acceptance options: any ID, specific ID, ID in dialup user group
- Supports IKEv1 and IKEv2 (RFC 4306)
- Authentication method: certificate and pre-shared key
- IKE mode configuration support (as server or client)
- DHCP over IPSEC
- Configurable IKE encryption key expiry, NAT traversal keep alive frequency
- Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
- Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
- Phase 1/Phase 2 Diffie-Hellman support: 1,2,5
- XAuth as server mode and for dialup users
- Dead peer detection
- Replay detection
- Auto key keep-alive for Phase 2 SA

• IPSEC VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
• IPSEC VPN configuration options: route-based or policy based
• IPSEC VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode
• One time login prevents concurrent logins with the same username
• SSL portal concurrent users limiting
• SSL VPN port forwarding module encrypts client data and sends the data to the application server
• Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS
• Host integrity checking and OS checking prior to SSL tunnel connections
• MAC host check per portal
• Cache cleaning option prior to ending SSL VPN session
• L2TP client and server mode, L2TP over IPSEC, and GRE over IPSEC
• View and manage IPSEC and SSL VPN connections
• PnPVPN

IPv6

• Management over IPv6, IPv6 logging and HA
• IPv6 tunneling, DNS64/NAT64 etc
• IPv6 routing protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
• IPS, Application identification, Access control, ND attack defense

VSYS

• System resource allocation to each VSYS
• CPU virtualization
• Non-root VSYS support firewall, IPSec VPN, SSL VPN, IPS, URL filtering
• VSYS monitoring and statistic

High Availability

• Redundant heartbeat interfaces
• Active/Active and Active/Passive
• Standalone session synchronization
• HA reserved management interface
• Failover:
- Port, local & remote link monitoring
- Stateful failover
- Sub-second failover
- Failure notification
• Deployment options:
- HA with link aggregation
- Full mesh HA
- Geographically dispersed HA

User and Device Identity

• Local user database
• Remote user authentication: TACACS+, LDAP, Radius, Active
• Single-sign-on: Windows AD
• 2-factor authentication: 3rd party support, integrated token server with physical and SMS
• User and device-based policies
• User group synchronization based on AD and LDAP
• Support for 802.1X, SSO Proxy

Administration

• Management access: HTTP/HTTPS, SSH, telnet, console
• Central Management :DCN Security Manager , web service APIs
• System Integration: SNMP, Syslog , alliance partnerships
• Rapid deployment: USB auto-install, local and remote script execution
• Dynamic real-time dashboard status and drill-in monitoring widgets
• Language support: English

Logs & Reporting

• Logging facilities: local memory and storage (if available), multiple syslog servers
• Encrypted logging and scheduled batch log uploading
• Reliable logging using TCP option (RFC 3195)
• Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets, URL etc.
• Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications
• IP and service port name resolution option
• Brief traffic log format option
• Three predefined reports: Security, Flow and network reports
• User defined reporting
• Reports can be exported in PDF via Email and FTP

Product Specification

Based on 5.0R4 FW				
Model	**N9040**	**M8420**	**N7210**	**N6008**
Hardware Specification				
DRAM Memory (Standard/Max)	16GB	8GB	2GB	2GB
Flash	512MB	512MB	512MB	512MB
Management Interface	1 x CON, 1 x AUX, 1 x USB2.0, 1 x HA, 1 x MGT	1 x CON, 1 x AUX, 1 x USB2.0, 1 x HA, 1 x MGT	1 x CON, 1 x AUX, 1 x USB2.0, 1 x HA, 1 x MGT	1 x CON, 1 x USB2.0
Phisical Interface	4 x 10/100/1000Base-T 4 x SFP	4 x 10/100/1000Base-T (Include two bypass ports) 4 x SFP 2 x SFP+	6 x 10/100/1000Base-T 4 x SFP	5 x 10/100/1000Base-T 4 x SFP/GE combo
Expansion Slot	4 expansion slot	4 expansion slot	2 expansion slot	NA
Expansion Module	MFW-1800E-8GT MFW-1800E-8GB MFW-1800E-4GT-B MFW-1800E-4GT-P MFW-N90-2XFP MFW-1800E-8SFP+	MFW-1800E-8GT MFW-1800E-8GB MFW-1800E-4GT-B MFW-1800E-4GT-P MFW-N90-2XFP MFW-1800E-8SFP+	MFW-1800E-8GT MFW-1800E-8GB MFW-1800E-4GT-B MFW-1800E-4GT-P	NA
Power	Dual hotswap power, 450W	Dual hotswap power, 450W	Dual redundant power, 150W	Dual redundant power, 45W
Power input	AC：100-240V，50/60Hz	AC：100-240V 50/60Hz	AC：100-240V 50/60Hz	AC: 100-240V，50/60Hz
Mounting	2U rackable	2U rackable	1U rackable	1U rackable
Dimension (WxDxH)	440.0mm×520.0mm×88.0mm	440.0mm×530.0mm×88.0mm	436.0mm×366.0mm×44.0mm	442.0mm×241.0mm×44.0mm
Weight	12.3KG	11.8kg	5.6kg	2.5kg
Working Temperature	0-40℃	0-40℃	0-40℃	0-40℃
Working Humidity	10-95%(non-condensing)	10-95%(non-condensing)	10-95%(non-condensing)	10-95%(non-condensing)

Model	N9040	N8420	N7210	N6008
Product Performance				
Throughtput (1518Byte)	40Gbps	20Gbps	10Gbps	8Gbps
Throughtput (64Byte)	10Gbps	5Gbps	1.5Gbps	400Mbps
IPSec Throughtput (1400Byte)	25Gbps	10Gbps	5Gbps	1Gbps
Anti-virus Throughtput	6Gbps	3Gbps	2Gbps	500Mbps
IPS Throughtput	8Gbps	4Gbps	3Gbps	1Gbps
Maximum Concurrent Connections	12 million	6 million	2 million	2 million
New Connections Per Second(HTTP)	500 thousand	200 thousand	100 thousand	50 thousand
New Connections Per Second(TCP)	600 thousand	300 thousand	150 thousand	80 thousand
Feature Parameters				
Max service/group entries	6000	6000	2048	512
Max policy entries	40000	40000	8000	2000
Max zone number	512	512	256	128
Max address entries per device(IPv4 Only version)	16384	8192	8192	4096
Max num of ipsec tunnels	20000	20000	6000	1000
Max Concurrent Users(Standard/Max)	8/10000	8/10000	8/4000	8/1000
Max routes(IPv4 Only version)	30000	30000	10000	4000
maximum VSYS supported	250	250	50	5
Max virtual router	250	250	50	5
Max num of gre tunnels	1024	1024	256	128

Based on 5.0R4 FW			
Model	**N5005**	**N3002**	**N2002**
Hardware Specification			
DRAM Memory（Standard/Max）	2GB	1GB	1GB
Flash	512MB	512MB	512MB
Management Interface	1 x CON, 1 x USB2.0	1 x CON, 1 x USB2.0	1 x CON, 1 x USB2.0
Phisical Interface	9 x 10/100/1000Base-T	9 x 10/100/1000Base-T	9 x 10/100/1000Base-T
Expansion Slot	NA	NA	NA
Expansion Module	NA	NA	NA
Power	Singal power, 45W	30W	30W
Power input	AC：100-240V，50/60Hz	AC：100-240V 50/60Hz	AC：100-240V 50/60Hz
Mounting	1U rackable	1U rackable	desktop mounting, not rackable
Dimension（WxDxH）	442.0mm×241.0mm×44.0mm	442.0mm×241.0mm×44.0mm	320.0mm x 150.0mm x 44.0mm
Weight	2.5kg	2.5kg	1.5kg
Working Temperature	0-40℃	0-40℃	0-40℃
Working Humidity	10-95%(non-condensing)	10-95%(non-condensing)	10-95%(non-condensing)
Product Performance			
Throughtput（1518Byte）	5Gbps	2Gbps	2Gbps
Throughtput（64Byte）	250Mbps	150Mbps	150Mbps
IPSec Throughtput（1400Byte）	800Mbps	500Mbps	500Mbps
Anti-virus Throughtput	120Mbps	100Mbps	100Mbps
IPS Throughtput	300Mbps	250Mbps	250Mbps

Model	N5005	N3002	N2002
Maximum Concurrent Connections	1 million	200 thousand	200 thousand
New Connections Per Second(HTTP)	20 thousand	10 thousand	10 thousand
New Connections Per Second(TCP)	30 thousand	20 thousand	20 thousand
Feature Parameters			
Max service/group entries	512	256	256
Max policy entries	1000	1000	1000
Max zone number	32	16	16
Max address entries per device(IPv4 Only version)	512	512	512
Max num of ipsec tunnels	512	512	512
Max Concurrent Users(Standard/Max)	8/500	8/128	8/128
Max routes(IPv4 Only version)	1024	512	512
maximum VSYS supported	NA	NA	NA
Max virtual router	2	2	2
Max num of gre tunnels	32	8	8