DCFW-1800E Series
Next-Generation Firewalls

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

User
Application
Content
Device
Deployment flexibility to protect all locations
Simple and consistent management

Model and Appearance of DCFW-1800E Series

Appearance	Description
 DCFW-1800E-N9040	Carrier-grade 10G Security Gateway 32Gbps Throughput 8Gbps Anti-virus Throughput 15Gbps IPS Throughput 12 million Concurrent Connections 50000 Concurrent Users 10000 SSL VPNs Recommended export bandwidth: 5Gbps
 DCFW-1800E-N8420	Carrier-grade Gigabit Security Gateway 16Gbps Throughput 3.5Gbps Anti-virus Throughput 5Gbps IPS Throughput 6 million Concurrent Connections 20000 Concurrent Users 10000 SSL VPNs Recommended export bandwidth: 1.5Gbps
 DCFW-1800E-N7210	Carrier-grade Gigabit Security Gateway 8Gbps throughput 1.6Gbps Anti-virus Throughput 3Gbps IPS Throughput 3 million Concurrent Connections 8000 Concurrent Users 4000 SSL VPNs Recommended export bandwidth: 800Mbps
 DCFW-1800E-N6008	Campus-grade Gigabit Security Gateway 4Gbps throughput 700Mbps Anti-virus throughput 1Gbps IPS Throughput 2 million Concurrent Connections 2000 Concurrent Users 1000 SSL VPNs Recommended export bandwidth: 350Mbps
 DCFW-1800E-N5005	SMB-grade Security Gateway 2Gbps throughput 400Mbps Anti-virus throughput 600Mbps IPS Throughput 1 million Concurrent Connections 800 Concurrent Users 500 SSL VPNs Recommended export bandwidth: 150Mbps
 DCFW-1800E-N3002	SMB-grade Security Gateway 1Gbps throughput 300Mbps Anti-virus throughput 400Mbps IPS Throughput 200 thousand Concurrent Connections 150 Concurrent Users 128 SSL VPNs Recommended export bandwidth: 80Mbps

 DCFW-1800E-N2002	SMB-grade Security Gateway with Wi-Fi 1Gbps throughput 300Mbps Anti-virus throughput 400Mbps IPS Throughput 200 thousand Concurrent Connections 150 Concurrent Users 128 SSL VPNs Recommended export bandwidth: 80Mbps

Key Features and Highlights

Granular Application Identification and Control

The DCFW-1800E 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-1800E 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, etc.), which significantly enhances the protection efficiency and reduces network latency.

Network Services

- Dynamic routing (OSPF, BGP, RIPv2)
- Static and Policy routing
- Route controlled by an 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, DCE/RPC, 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 an 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 the administrator to temporarily assign different profiles to user/group/IP
- Web filter local categories and category rating override

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 2 operation systems
- Support query based on IP and endpoint quantity

File Transfer Control

- File transfer control based on the 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 a 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
- Autokey 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 before SSL tunnel connections
- MAC host check per portal
- Cache cleaning option before 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
• 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

Specifications

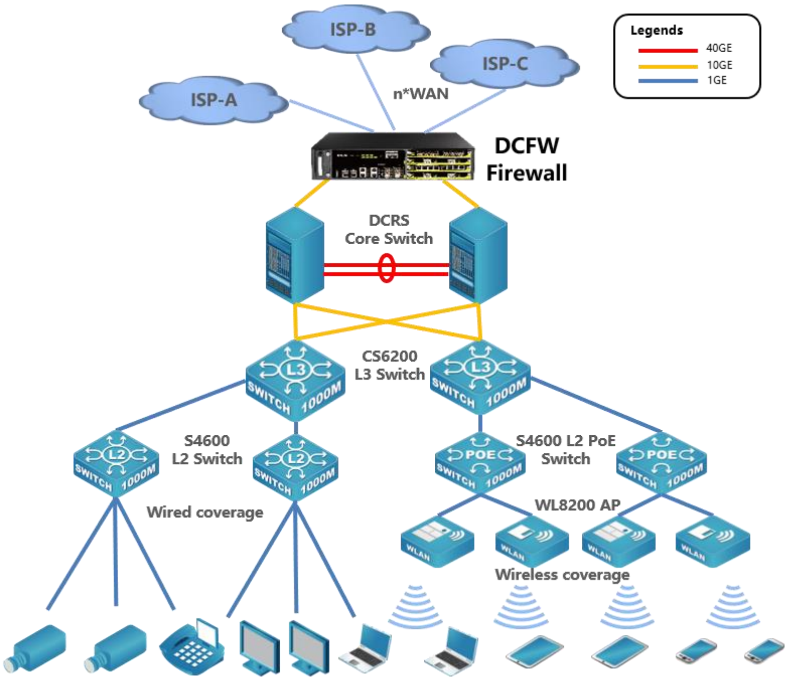
Model	N9040	N8420	N7210	N6008
Hardware Specification				
DRAM Memory (Standard/Max)	16GB	8GB	2GB	2GB
Flash	512MB			
Management Interface	1*Console, 1*AUX, 1*USB2.0, 1*HA, 1*MGT			1*Console, 1*USB2.0

Physical Interface	4*GE RJ45 4*GE SFP	4*GE RJ45 (2*Bypass ports included) 4*GE SFP 2*10GE SFP+	6*GE RJ45 4*GE SFP	5*GE RJ45 4* SFP/GE combo
Expansion Slot	4		2	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 hot-swappable, 450W		Dual fixed, 150W	Dual fixed, 45W
Voltage Range	100-240V AC, 50/60Hz			
Mounting	2U rack		1U rack	
Dimension (W x D x H)	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℃			
Working Humidity	10-95%(non-condensing)			
Product Performance				
Throughput (Standard/max)	32Gbps	16Gbps	8Gbps	2.5/4Gbps
IPSec Throughput	18Gbps	8Gbps	3Gbps	1Gbps
Anti-virus Throughput	8Gbps	3.5Gbps	1.6Gbps	700Mbps
IPS Throughput	15Gbps	5Gbps	3Gbps	1Gbps
Concurrent Connections (Standard/Max)	12M	6M	3M	1M/2M
New HTTP Connections per second	340K	150K	75K	26K
New TCP Connections per second	500K	200K	120K	50K
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 IPv4 address entries	16384	8192	8192	4096
Max IPsec tunnels	20000	20000	6000	2000
Concurrent Users (Standard/Max)	8/50000	8/20000	8/8000	8/2000
SSL VPN connection (Standard/Max)	8/10000	8/10000	8/4000	8/1000
Max routes (IPv4 Only version)	30000	30000	10000	4000
Max VSYS supported	250	250	50	5
Max virtual router	250	250	50	5
Max GRE tunnels	1024	1024	256	128

Model	N5005	N3002	N2002
Hardware Specification			
DRAM Memory（Standard/Max）	2GB	1GB	1GB
Flash	512MB		
Management Interface	1*Console, 1*USB2.0		
Physical Interface	9*GE RJ45		
Expansion Slot	NA		
Expansion Module	NA		
Power	Single power, 45W	30W	30W
Voltage Range	100-240V AC, 50/60Hz		
Mounting	1U rack		desktop
Dimension（WxDxH）	442.0mm×241.0mm ×44.0mm	442.0mm×241.0mm ×44.0mm	320.0mmx150.0mm x 44.0mm
Weight	2.5kg	2.5kg	1.5kg
Working Temperature	0-40℃		
Working Humidity	10-95%(non-condensing)		
Product Performance			
Throughput（Standard/Max）	1.5/2Gbps	1Gbps	1Gbps
IPSec Throughput	700Mbps	600Mbps	600Mbps
Anti-virus Throughput	400Mbps	300Mbps	300Mbps
IPS Throughput	600Mbps	400Mbps	400Mbps
Concurrent Connections (Standard/Max)	600K/1M	200K	200K
New HTTP Connections per second	15K	8K	8K
New TCP Connections per second	25K	10K	10K
Feature Parameters			
Max service/group entries	512	256	256
Max policy entries	1000	1000	1000
Max zone number	32	16	16
Max IPv4 address entries	512	512	512
Max IPsec tunnels	2000	512	512
Concurrent Users (Standard/Max)	8/800	8/150	8/150
SSL VPN connection（Standard/Max）	8/500	8/128	8/128
Max routes (IPv4 Only version)	1024	512	512
Max VSYS supported	NA		
Max virtual router	2	2	2
Max GRE tunnels	32	8	8

Typical Application

For enterprises and service providers, DCFW-1800E NGFW can manage all of their security risks with the industry's best-of-breed IPS, SSL inspection, and threat protection. The DCFW-1800E series can be deployed at the enterprise edge, the hybrid data center, and across internal segments. The multiple high-speed interfaces, high port density, superior security efficacy, and high throughput of this series keep your network connected and secure.



Order Information

NGFW Firewall	
DCFW-1800E-N9040	Carrier-class high-end 10G security gateway Maximum expansion to 42 x 1G interfaces, 16 x 10G interfaces. Default with 4 x 10/100/1000 Base-T ports, 4 x 1G SFP ports, one HA interface, one management port, four expansion slots, hot-swap dual power supply redundancy design.
DCFW-1800E-N8420	Carrier-class high-end Gigabits security gateway Maximum expansion to 42 x 1G interfaces, 18 x 10G interfaces. Default with 4 x 10/100/1000 Base-T ports (Include two bypass ports), 4 x 1G SFP ports, 2 x SFP+ ports, one HA interface, one management port, four expansion slots, hot-swap dual power supply redundancy design.
DCFW-1800E-N7210	Carrier-class high-end Gigabits security gateway Maximum expansion to 28 x 1G interfaces. Default with 6 x 10/100/1000 Base-T ports, 4 x 1G SFP ports, one HA interface, one management port, two expansion slots, hot-swap dual power supply redundancy design.
MFW-1800E-8GT	8 x 10/100/1000 Base-T ports module, could be used on N9040, N8420, and N7210.
MFW-1800E-8GB	8 x 1G SFP ports module, could be used on N9040, N8420 and N7210.
MFW-1800E-4GT-B	4 x 10/100/1000 Base-T ports bypass module, could be used on N9040, N8420, and N7210.

MFW-1800E-4GT-P	4 x 10/100/1000 Base-T ports PoE module, could be used on N9040, N8420, and N7210.
MFW-N90-2XFP	2 x 10G XFP ports model, could be used on N9040 and N8420.
MFW-N90-4XFP	4 x 10G XFP ports model, could be used on N9040 and N8420.
MFW-1800E-8SFP+	8 x 10G SFP+ ports model, could be used on N9040 and N8420.
DCFW-1800E-N6008	Large campus-level Gigabit security gateway 5 x 10/100/1000M Base-T ports, 4 Gigabit Combo ports, dual power supply redundancy design
DCFW-1800E-N5005	Small and medium enterprise-class security gateway 9 x 10/100/1000M Ethernet ports, 1U
DCFW-1800E-N3002	Small and medium enterprise-class security gateway 9 x 10/100/1000M Ethernet ports, 1U
DCFW-1800E-N2002	Small enterprise-class security gateway 9 x 10/100/1000M Ethernet ports, integrated Wi-Fi module, support external 3G module, 1U desktop box, could not be installed on a 19-inch rack.
License for NGFW	
DCFW-SSL-License-10	DCFW-SSL-License for 10 users (Need to be used with security gateway)
DCFW-SSL-License-50	DCFW-SSL-License for 50 users (Need to be used with security gateway)
DCFW-SSL-License-100	DCFW-SSL-License for 100 users (Need to be used with security gateway)
DCFW-SSL-UK10	10 SSL VPN hardware USB Key (Need to be used with security gateway)
USG-N9040-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N9040 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N9040-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N9040 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license
USG-N8420-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N8420 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N8420-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N8420 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license

USG-N7210-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N7210 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N7210-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N7210 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license
USG-N6008-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N6008 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N6008-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N6008 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license
USG-N5005-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N5005 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N5005-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N5005 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license
USG-N3002-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N3002 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license
USG-N3002-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N3002 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license
USG-N2002-LIC-3Y	3 years upgrade license of all USG feature library for DCFW-1800E-N2002 Including: 3 years virus database upgrade license 3 years URL classification library upgrade license 3 years IPS feature library upgrade license 3 years application feature library upgrade license

USG-N2002-LIC	1-year upgrade license of all USG feature library for DCFW-1800E-N2002 Including: 1-year virus database upgrade license 1-year URL classification library upgrade license 1-year IPS feature library upgrade license 1-year application feature library upgrade license