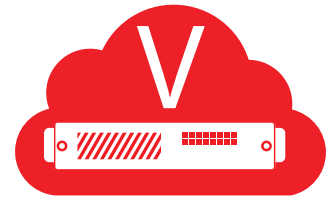# FIREBOX**V**

Best-in-Class Network Security for Your Virtual Environment

Organizations of all sizes are turning to virtualization to reduce costs and increase the efficiency, availability, and flexibility of their IT resources. But virtualization comes at a cost. Virtual environments are complex to manage and vulnerable to security threats. IT must be prepared. Now applications can be secured, resources can be maximized, and your IT department can reap the rewards of having a single, unified management system – without a security risk in sight. WatchGuard FireboxV brings best-in-class network security to the world of virtualization. With real-time monitoring, multi-WAN support, and scalable solutions to fit any-sized business, your virtual environments can be just as secure as your physical one.

WatchGuard's virtual solutions provide you with unmatched deployment flexibility. You can choose to deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform. WatchGuard virtual appliances feature all of the security and networking services found in our physical appliances and can be deployed in a per-customer, -department, or -app scenarios, for your virtual infrastructure.

Virtualize the Traditional Gateway Firewall for Unprecedented Flexibility

WatchGuard FireboxV protects not only the physical perimeter of the datacenter, but the "virtual edge." Now you can easily implement policy that protects the data in the corporate database from the messaging infrastructure, or confidential HR information from financial data from other divisions – even when running on the same servers.

Consolidate Multiple Firewalls for High-Impact Efficiencies

Service providers – hosting, Cloud, or managed security services – can deploy multiple instances of FireboxV on servers at the perimeter of their datacenters. These virtual firewalls are isolated from each other, so service level agreements (SLAs) can be guaranteed to each tenant, and a configuration change to one doesn't affect the others. And yet they can all be managed by the provider using a single intuitive console.

Eliminate Redundant Hardware Costs While Securing the Virtual Networks – Branch Consolidation

As larger branches and divisions consolidate local servers – file, print, voice, and more – onto one box, a virtual firewall can be deployed on the physical server, insulating all traffic from the public Internet. A single VPN tunnel can provide a secure path back to corporate datacenters or virtual private clouds – yielding cost savings at every location without compromising security.

Features & Benefits

- Run virtual appliances on your virtual environment
- Leading UTM/NGFW features and services in virtual infrastructure
- Visibility with WatchGuard Cloud and on-premises Dimension, a public and private cloud-ready visibility solution, instantly turns raw data into security intelligence – included with the purchase
- Easy to download, enable, deploy, and manage (centralized console, web UI, CLI)
- Leverages vSphere and Hyper-V flexibility and availability
- Multiple models for organizations of all sizes
- WatchGuard's innovative HTML5 Access Portal provides a secure singlesign-on (SSO) experience over TLS 1.2.
- Per-customer, -department, or -app deployment

FireboxV

FireboxV	MICRO	SMALL	MEDIUM	LARGE	XLARGE
TECHNICAL SPECIFICATIONS					
CPU Core Limit	2	2	4	8	16
User Count	5	50	250	750	1,500
EDR Core Licenses	5	50	150	250	250
Firewall	1 Gbps	2 Gbps	4 Gbps	8 Gbps	Unrestricted
VPN	0.2 Gbps	0.4 Gbps	1.5 Gbps	3.0 Gbps	Unrestricted
BOVPN Tunnels	5	50	600	6,000	10,000
VLANs	10	50	300	750	1,500

SECURITY FEATURES

|	
Firewall	Stateful packet inspection, deep packet inspection, proxy firewall
Application proxies	HTTP, HTTPS, FTP, DNS, TCP/UDP, POP3S, SMTPS, IMAPS and Explicit Proxy
Threat protection	DoS attacks, fragmented packets, blended threats and more
Filtering options	Browser Safe Search, YouTube for Schools, Google for Business
Security subscriptions	APT Blocker, IPS, Gateway AV, WebBlocker, App Control, Reputation Enabled Defense, spamBlocker, Network Discovery, Threat Detection and Response, Access Portal

STANDARD NETWORKING

Hypervisor Support	• VMware ESXi 6.5, 6.7, 7.0, or 8.0 • Hyper-V for Microsoft Windows Server 2019 or 2022, and Hyper-V Server 2019 • KVM in CentOS 8.1
QoS	8 priority queues, DiffServ, modified strict queuing
IP address assignment	DHCP (client)
NAT	Static, dynamic, 1:1, IPSec traversal
Other features	Static routing, port Independence

VPN & AUTHENTICATION

Encryption	DES, 3DES, AES 128-, 192-, 256-bit
IPSec	SHA-2, IKE pre-shared key, 3rd party cert, IKEv1/v2, Suite B
Single sign-on	Windows, macOS, mobile operating systems, RADIUS, SAML 2.0
Authentication	RADIUS, LDAP, Windows Active Directory, RSA SecurID, internal database, SAML 2.0

MANAGEMENT

Logging and notifications	WatchGuard, Syslog, SNMP v2/v3
User interfaces	WebUI, scriptable CLI
Reporting	WatchGuard Dimension includes over 100 pre-defined reports, executive summary and visibility tools
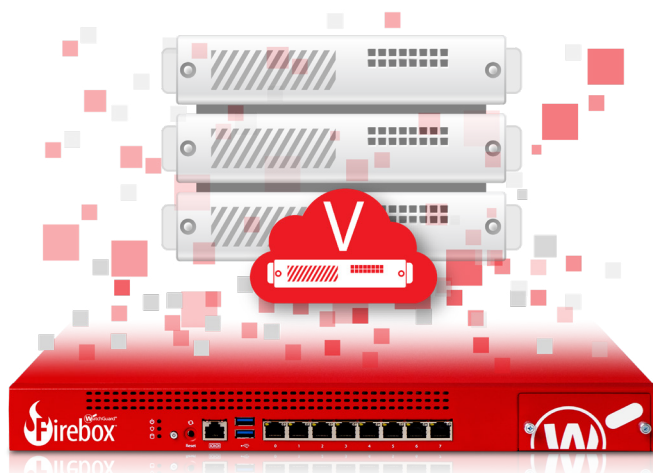
Strong Security at Every Layer

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions deliver in-depth defenses against advanced malware, ransomware, botnets, trojans, viruses, drive-by downloads, phishing and much more.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service (IPS)		✓	✓
Application Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
DNSWatch			✓
IntelligentAV**			✓
ThreatSync (XDR)			✓
EDR Core			✓

WatchGuard Cloud
    Log Data Retention
    Report Data Retention
		90 Days
		1 Day
			365 Days
			30 Days

Support	Standard (24 x 7)	Standard (24 x 7)	**Gold (24 x 7)**

*Not available on Firebox T20/T20-W, T25/T25-W, or T35-R. Total Security Suite required for M270, M370, M470, M570, M670, FireboxV and Firebox Cloud.
**Not available on Firebox T20/T20-W, T25/T25-W, or T35-R.

Multiple Purchase Options

The flexibility of WatchGuard's integrated platform makes it easy to have exactly the security components your business network requires. Whether you choose to start with the security basics or deploy a comprehensive arsenal of network defenses, we have bundled security services to match your requirements.

Expert Guidance and Support

An initial Support subscription comes with every FireboxV model. Standard Support, which is included in the Basic Security Suite, provides 24 x 7 technical support and software updates. An upgrade to Gold level support is included in WatchGuard's Total Security Suite.

The WatchGuard Portfolio

Network Security

Multi-Factor Authentication

Secure Cloud Wi-Fi

Endpoint Security

Contact your authorized WatchGuard reseller or visit **www.watchguard.com** to learn more.