SECURITY FOR
SMALL BUSINESSES
UNCOMPROMISING PERFORMANCE
A common problem with firewalls used by small businesses has to do with hardware performance. Most often, vendor-stated bandwidth claims fall short when put to the real-world test. As a result, as Internet speeds degrade over time, security services are often disabled to compensate. This action allows entry for Internet attacks. Check Point security gateways for small businesses provide unparalleled security without the performance degradation witnessed by other firewalls. Small businesses are able to maintain full Internet performance without disabling key security features.

SECURITY WITHOUT COMPLEXITY
Many small businesses need protection against today’s sophisticated cyber-attacks and zero-day threats. Check Point security gateways for small businesses bring the same protection used by large enterprises and Fortune 100 companies and make it easily accessible. The same next-generation threat prevention deployed to deliver the highest levels of protection for large enterprises integrates firewall, VPN, antivirus, anti-bot, application visibility and control, URL filtering, email security and SandBlast Zero-Day Protection (sandboxing) in a simpler, easy-to-use, easy-to-manage small business package.

Ready to Use Pre-defined Security Policy
COMPREHENSIVE THREAT PREVENTION
The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats requires a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention to combat these emerging threats while reducing complexities and increasing operational efficiencies. The Check Point Threat Prevention solution includes powerful security features such as firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known cyber-attacks and threats – now enhanced with the award-winning SandBlast™ Threat Emulation for complete protection against the most sophisticated threats and zero-day vulnerabilities.

PREVENT KNOWN AND ZERO-DAY THREATS
As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.
QUANTUM SPARK 1600, 1800

UNCOMPROMISING PERFORMANCE

OVERVIEW

Enforcing consistent network security is challenging for small to mid-size businesses where there are few users with little to no IT expertise. Small to mid-size business offices require the same level of protection from sophisticated cyber-attacks and zero-day threats that is available in larger enterprise offices.

The Check Point Quantum Spark 1600 and 1800 security gateways deliver enterprise-grade security in simple, affordable, all-in-one security solutions in a 1 Rack Unit (RU) form factor to protect small to mid-size business employees, networks and data from cyber-theft. High threat prevention throughput and high port capacity with 2.5 and 10 GbE network interfaces in the 1800 make these NGFWs ideal for larger branch and SMB networks.

ALL-INCLUSIVE SECURITY

The 1600 and 1800 gateways come standard with sixteen (16) 1-Gigabit Ethernet LAN switch ports and a 1-GbE WAN port configuration that supports copper or fiber connections. The DMZ port is a combination copper/fiber 1 GbE port in the 1600 and 10 GbE in the 1800. The 1800 has an additional two (2) 2.5 GbE LAN ports and two (2) power supplies for redundancy.

1600, 1800 GATEWAY HIGHLIGHTS

<table>
<thead>
<tr>
<th>Maximum Capacities</th>
<th>1600</th>
<th>1800</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat prevention</td>
<td>1.5 Gbps</td>
<td>2 Gbps</td>
</tr>
<tr>
<td>Next-Gen Firewall + IPS</td>
<td>3.2 Gbps</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>LAN ports</td>
<td>16x 1GbE copper ports</td>
<td>16x 1GbE copper plus 2x 2.5GbE copper ports</td>
</tr>
<tr>
<td>WAN ports</td>
<td>1x 1GbE copper/fiber port</td>
<td>2x 1GbE copper/fiber port</td>
</tr>
<tr>
<td>DMZ ports</td>
<td>1x 1GbE copper/fiber port</td>
<td>1x 10GbE copper/fiber port</td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>2 redundant</td>
</tr>
<tr>
<td>Storage</td>
<td>32 GB eMMC plus a 64 GB micro-SD card option</td>
<td>32 GB eMMC plus a 256 GB SSD</td>
</tr>
</tbody>
</table>

*measured with an Enterprise traffic blend and the most secure threat prevention
Enforcing consistent network security is challenging in small offices and where the enterprise border extends to small, remote and branch offices where there are a few users with little to no IT expertise. Small and remote offices require the same level of protection from sophisticated cyber-attacks and zero-day threats as main corporate offices.

The Quantum Spark 1500 security gateways are ideal for small and remote branch offices. For local management and support in a small office environment, an easy and intuitive web-based local management interface is available. Enterprises who want to manage security from a central office can leverage on-premises or cloud-hosted security management to remotely manage and apply a consistent security policy to thousands of devices across the field offices.

### ALL-INCLUSIVE SECURITY

All-Inclusive Next Generation Threat Prevention (NGTP) with SandBlast: apply multiple layers of protection to prevent sophisticated cyber-threats — with Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Email Security and SandBlast Zero-Day Protection (sandboxing).

### 1500 GATEWAY HIGHLIGHTS

Available in four models, the 1530/1550 and the 1570/1590, these gateways come standard with six (6) or ten (10) 1-Gigabit Ethernet ports respectively. Models with Wi-Fi, Wi-Fi with xDSL and Wi-Fi with an embedded 3G/4G/LTE modem fit seamlessly into your home and branch office networks.

<table>
<thead>
<tr>
<th>Maximum Capacities</th>
<th>1530</th>
<th>1550</th>
<th>1570</th>
<th>1590</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat prevention</td>
<td>340 Mbps</td>
<td>450 Mbps</td>
<td>500 Mbps</td>
<td>660 Mbps</td>
</tr>
<tr>
<td>Next-Gen Firewall + IPS</td>
<td>600 Mbps</td>
<td>800 Mbps</td>
<td>970 Mbps</td>
<td>1,300 Mbps</td>
</tr>
<tr>
<td>1 GbE ports (Copper)</td>
<td>1x WAN, 5x LAN switch ports</td>
<td>1x WAN, 1x DMZ, 8x LAN switch ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fiber option</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Wi-Fi option</td>
<td>802.11 b/g/n/ac, 2.4 or 5GHz band</td>
<td>802.11 b/g/n and 802.11 n/ac wave II, 2.4 and 5 GHz bands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSL option</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>LTE option</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

*measured with an Enterprise traffic blend and the most secure threat prevention*
QUANTUM SPARK COMPARISON

<table>
<thead>
<tr>
<th></th>
<th>1530</th>
<th>1550</th>
<th>1570</th>
<th>1590</th>
<th>1600</th>
<th>1800</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat prevention (Mbps)</td>
<td>340</td>
<td>450</td>
<td>500</td>
<td>660</td>
<td>1,500</td>
<td>2,000</td>
</tr>
<tr>
<td>Next-Gen Firewall (Mbps)</td>
<td>600</td>
<td>800</td>
<td>970</td>
<td>1,300</td>
<td>3,200</td>
<td>5,000</td>
</tr>
<tr>
<td>Firewall throughput (Mbps)</td>
<td>1,000</td>
<td>1,000</td>
<td>2,800</td>
<td>2,800</td>
<td>4,800</td>
<td>7,500</td>
</tr>
<tr>
<td><strong>Ideal Test Conditions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall 1518 byte UDP (Mbps)</td>
<td>2,000</td>
<td>2,000</td>
<td>6,400</td>
<td>6,400</td>
<td>8,000</td>
<td>17,000</td>
</tr>
<tr>
<td>VPN AES-128 (Mbps)</td>
<td>970</td>
<td>1,300</td>
<td>1,950</td>
<td>2,600</td>
<td>3,200</td>
<td>4,000</td>
</tr>
<tr>
<td>Connections per second</td>
<td>10,500</td>
<td>14,000</td>
<td>15,750</td>
<td>21,000</td>
<td>55,000</td>
<td>66,000</td>
</tr>
<tr>
<td>Concurrent connections</td>
<td>500,000</td>
<td>500,000</td>
<td>500,000</td>
<td>500,000</td>
<td>2,400,000</td>
<td>2,400,000</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Email Security and SandBlast Threat Emulation (sandboxing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unicast, Multicast Routing</td>
<td>OSPFv2, BGPv4 and 4++, RIP, IGMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Access User License</td>
<td>100</td>
<td>100</td>
<td>200</td>
<td>200</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN ports</td>
<td>5x 1GbE</td>
<td>5x 1GbE</td>
<td>8x 1GbE</td>
<td>8x 1GbE</td>
<td>16x 1GbE</td>
<td>16x 1GbE</td>
</tr>
<tr>
<td>LAN ports, 2.5GbE</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>2x LAN</td>
</tr>
<tr>
<td>WAN ports</td>
<td>1x 1GbE</td>
<td>1x 1GbE</td>
<td>1x copper/fiber</td>
<td>1x copper/fiber</td>
<td>1x copper/fiber</td>
<td>2x copper/fiber</td>
</tr>
<tr>
<td>DMZ ports</td>
<td>x</td>
<td>x</td>
<td>1GbE</td>
<td>1GbE</td>
<td>1GbE</td>
<td>10GbE</td>
</tr>
<tr>
<td>Wi-Fi (optional)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>DSL (optional)</td>
<td>x</td>
<td>x</td>
<td>√</td>
<td>√</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>LTE modem (optional)</td>
<td>x</td>
<td>x</td>
<td>√</td>
<td>√</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Console port</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>USB ports</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SD card slot</td>
<td>x</td>
<td>x</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>SSD</td>
<td>x</td>
<td>x</td>
<td>√</td>
<td>√</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Power supplies</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Datasheet link</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*measured with enterprise traffic blend, the most secure threat prevention and logging enabled*
LACK THE EXPERTISE OR TIME FOR SECURITY?
Check Point and our partners offer a cloud managed security service that will oversee the ongoing operation of the Small Business Gateways. Security experts from Check Point or a Managed Security Service Provider (MSSP) manage security at a very low monthly cost, allowing small business owners to focus on growing their business.

The Cloud-Managed Security Service offers a simple, all-in-one solution with easy setup.
- Ongoing management through the cloud by Check Point security experts
- Continuous automatic security updates and upgrades
- 24x7 customer support by Check Point’s award-winning support team
- Security reports on demand or as requested

WHAT ARE YOU WAITING FOR?
Security for a small business is too important to ignore. With Check Point, small businesses can feel confident that they have the best security available, in a package that doesn’t require extensive expertise or time to get high levels of protection.

Contact a Check Point Authorized Reseller today to get started with enterprise-level security that protects the small business.

Visit www.checkpoint.com/smb for more information.