Huawei Eudemon1000E-N
Next-Generation Firewall

With the popularity of mobile working using smartphones and tablets, mobile apps, Web2.0, and social networking become integral parts of works. This change in IT environments greatly improves the communication efficiency but blurs network borders and makes information security more challenging. Traditional security gateway implements security control only based on IP addresses and ports, and cannot cope with the ever-increasing application layer and web threats.

Against this background, Huawei launches the Eudemon1000E-N series next-generation firewall to address these challenges. With the awareness of applications, time, users, attacks, and locations, the Eudemon1000E-N series clearly maps the network environment to service environment and provides application- and user-based security management and QoS management functions. Based on application identification, the Eudemon1000E-N series provides powerful IPS, AV capabilities to efficiently and comprehensively secure information.

Application protection is the core of the next-generation security. Configuring and managing application protection require more administrators with higher skills, increasing maintenance costs. However, the Eudemon1000E-N series eliminates such concerns by using the industry-leading SmartPolicy technology to automatically generate security policies based on the service awareness result, making next-generation security simple, consistent, and cost-effective.
## Features and Highlights

### Granular Application Access Control

In the Web2.0 era, social networking and IM applications are widely used for communication and information sharing on Internet. Massive applications are used, and most of them use the same protocol (HTTP) and the same port. Traditional firewalls are aware of IP addresses and ports, but not of user information, service environment, and application-layer information. However, awareness is the basis of access control and security protection. Firewalls require comprehensive context awareness to effectively take actions and protect information security.

Huawei Eudemon1000E-N series next-generation firewall analyzes internet service traffic from multi-dimensions, including application, time, user, attack, and location and implements comprehensive network protection.

- **Application**: Identifies 6000+ mobile and web applications using technologies, such as feature identification, port identification, correlation identification, and behavior identification. Application awareness, coupled with antivirus scanning, can recognize traffic of different applications and detect the viruses, Trojan horses, and malware hidden in applications.

- **User**: Supports eight user authentication methods, including RADIUS, LDAP, and AD authentication to associate traffic IP addresses and ports with users for per-user traffic control.

- **Threat**: Provides over 5000 signatures for attack identification. The Eudemon1000E-N series defends against web application attacks, such as cross-site scripting and SQL injection attacks, identifies and defends against more than 10 types of DDoS attacks, including SYN flood and UDP flood attacks, and identifies more than 5,000,000 viruses. With cloud-based URL filtering enabled, the Eudemon1000E-N series provides over 85,000,000 predefined URLs to block malicious websites.

- **Time**: Records the time when traffic anomalies or security events occur to provide evidence for audit.

- **Location**: Identifies the location where the traffic is initiated to implement differentiated traffic control in different regions. The Eudemon1000E-N series supports location customization based on IP addresses.

Based on the Context-awareness system, the Eudemon1000E-N series next-generation firewall accurately identifies threats hidden in applications and implements granular access control and network protection.

### Easy Security Management

Traditional security gateways and most next-generation firewalls can only passively execute policies configured by administrators. However, in the real world, attacks are usually a step ahead of network administrators. Therefore, completely relying on administrators cannot protect network security in the long run. However, Huawei Eudemon1000E-N series next-generation firewall can proactively discover network risks and dynamically generate protection and optimizing advises, like a security consultant. Proactive functions of security appliances are better than completely relying on administrators in the long run.
Compared with the traditional security gateways, the next-generation firewall features granular application control and in-depth application protection. Compared with traditional firewalls, using 5-tuple-based policies on the next-generation firewall does not improve network security. Next-generation firewalls have more powerful functions. However, configuring and managing these functions require more administrators with higher skills, which means a higher operation cost.

The Eudemon1000E-N series resolves this issue using the SmartPolicy technology. After automatic traffic pattern learning, the Eudemon1000E-N automatically generates security policies using the predefined knowledge base. Enterprise administrators need only a confirmation before the firewall applies the policies to the network. The SmartPolicy function decreases the TCO by 30% using the following functions:

- Dynamically discover security risks and automatically generate police tuning suggestions.
- Discover invalid and redundant policies to remove them.

**Excellent Performance**

Nowadays, hackers are launching organized attacks for illegal gains. Therefore, in-depth application protection, such as application-layer access control and intrusion prevention, becomes a must for network protection. However, the throughput of UTM devices is poor when application-layer protection is enabled.
In contrast, the Eudemon1000E-N series uses the Intelligent Awareness Engine (IAE) to implement Layer-7 protection and still deliver a throughput of a Layer-4 gateway. The traditional threat detection engine implements per-packet inspection and is easy to evade. The IAE analyzes and processes multiple services concurrently. The hardware acceleration module conducts core application analysis and signature matching, concurrently processing each security services, and updates the security status. This structure ensures the minimum compromise of the overall performance with multiple security services enabled. In terms of hardware, the Eudemon1000E-N series uses the dedicated multi-core platform for parallel processing. In addition, it uses the hardware acceleration technology and the content security acceleration chip on the CPU to function with the IAE for higher detection efficiency. The combination of the intelligent awareness engine and the elastic hardware structure enable the Eudemon1000E-N series to deliver 10-Gigabit level threat prevention performance, meeting the security protection requirements of large data centers.

Prevention of Unknown Threats
Unknown threats refer to the threats whose signatures are not yet extracted. These threats attack networks mainly through email and web access. Unknown attacks may occur when a user downloads a malicious email attachment, clicks a malicious URL link in an email message, executes a malicious script, or downloads a malicious file. However, the security devices cannot detect such attacks because they have no signatures to match them.

To address this issue, Huawei Eudemon1000E-N series next-generation firewall uses the Power Fortress Cloud detection system to detect unknown threats, and prevent Advanced Persistent Threat (APT) attacks. This system simulates suspicious samples collected around the world in the cloud sandbox and virtualization system to analyze these samples, including behavior analysis and service awareness, to detect viruses, 0-day attacks, phishing websites, botnets, and malicious websites. If any threat is found in a sample, the system further identifies the threat by IP address, domain name, file, URL, location, spam, user IP, and history. Then the system updates the global reputation detection and query system in the cloud. With 7 x 24 pushing service of the Power Fortress Cloud-U cloud center for security knowledge base updates, the Eudemon1000E-N series can obtain the latest threat detection and prevention capability to effective defend against unknown threats.

Typical Application Scenarios

Network Isolation and VPN Interconnection
- Challenges for customers: Network areas are not clearly divided, access control is insufficient, and the data transmitted between mobile employees or branches and the headquarters is likely to be intercepted or tampered.
- Highlights of the solution: delivers high throughput to avoid bottleneck at network borders, supports security zones to clearly divide networks, offers flexible packet filtering policies to accurately control communication, and encapsulates and checks packets of VPN users to ensure the security of data communication.
External Threat Prevention

- Challenges for customers: Coming along with the abundant Internet resources are threats such as DDoS attacks, malicious intrusions, and viruses.
- Highlights of the solution: The capabilities of supporting large numbers of concurrent connections and new connections per second help to combat the numerous DDoS attacks. Empowered by advanced IPS and anti-virus technologies as well as vulnerability-based and real-time updated signature database, the Eudemon1000E-N series implements near-zero false positives and negatives and a detection ratio of higher than 99%; defends against diversified threats from the Internet, and ensures the security of the intranet.

Online Behavior Management

- Challenges for customers: None-work-related Internet surfing, P2P download, online games, and stock transaction waste bandwidths for business, reduce employee productivity, and pose potential risks from malicious codes and hacker attacks.
• Highlights of the solution: The Eudemon1000E-N series provides over 6000 of identifiable applications, providing visibility into the applications running on your network. The URL database containing 8.5 million website URLs helps to shield against Trojan horse-embedded and phishing sites, block pornographic and gambling sites, regulate employee online behaviors and prevent them from engaging in activities that would harm internal network security. Multi-dimensional control measures based on users, applications, time, and bandwidth ensure bandwidth for mission-critical services and improve the bandwidth usage. You can work more efficiently and have P2P, IM, game sites, and other websites under control.

## Product Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>Eudemon 1000E-N3</th>
<th>Eudemon 1000E-N5</th>
<th>Eudemon 1000E-N6</th>
<th>Eudemon 1000E-N7</th>
<th>Eudemon 1000E-N7E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall throughput</td>
<td>10Gbit/s</td>
<td>20Gbit/s</td>
<td>30Gbit/s</td>
<td>40Gbit/s</td>
<td>40Gbit/s</td>
</tr>
<tr>
<td>IPS throughput</td>
<td>5Gbit/s</td>
<td>5.8Gbit/s</td>
<td>8Gbit/s</td>
<td>8.8Gbit/s</td>
<td>15Gbit/s</td>
</tr>
<tr>
<td>IPS+AV throughput</td>
<td>4Gbit/s</td>
<td>5Gbit/s</td>
<td>7Gbit/s</td>
<td>8Gbit/s</td>
<td>13Gbit/s</td>
</tr>
<tr>
<td>Maximum concurrent sessions</td>
<td>6,000,000</td>
<td>6,000,000</td>
<td>10,000,000</td>
<td>10,000,000</td>
<td>12,000,000</td>
</tr>
<tr>
<td>New sessions/second</td>
<td>200,000</td>
<td>250,000</td>
<td>350,000</td>
<td>400,000</td>
<td>400,000</td>
</tr>
<tr>
<td>VPN Throughput (IPSec, 3DES)</td>
<td>8Gbit/s</td>
<td>12Gbit/s</td>
<td>18Gbit/s</td>
<td>18Gbit/s</td>
<td>18Gbit/s</td>
</tr>
<tr>
<td>Maximum connections of IPSec</td>
<td>15,000</td>
<td>15,000</td>
<td>15,000</td>
<td>15,000</td>
<td>15,000</td>
</tr>
<tr>
<td>SSL VPN Maximum concurrent users</td>
<td>2000</td>
<td>2000</td>
<td>5000</td>
<td>5000</td>
<td>5000</td>
</tr>
<tr>
<td>MTBF</td>
<td>16.78years</td>
<td>16.78years</td>
<td>27.07years</td>
<td>23.67years</td>
<td>19.18years</td>
</tr>
</tbody>
</table>

## Physical Specifications

<table>
<thead>
<tr>
<th>Fixed Interface</th>
<th>8GE+4SFP</th>
<th>8GE+4SFP</th>
<th>2*10GE+8GE+8SFP</th>
<th>4*10GE+16GE+8SFP</th>
<th>4*10GE+16GE+8SFP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slots</td>
<td>2WSIC</td>
<td>2WSIC</td>
<td>6WSIC</td>
<td>5WSIC</td>
<td>5WSIC</td>
</tr>
<tr>
<td>Interface card type</td>
<td>2×10GE (SFP+) + 8×GE (RJ45), 8×GE (RJ45), 8×GE (SFP), 4×GE (RJ45) BYPASS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Height</td>
<td>1U</td>
<td>1U</td>
<td>3U</td>
<td>3U</td>
<td>3U</td>
</tr>
<tr>
<td>Dimensions (H x W x D)</td>
<td>442<em>421</em>43.6</td>
<td>442<em>421</em>43.6</td>
<td>442<em>415</em>130.5</td>
<td>442<em>415</em>130.5</td>
<td>442<em>415</em>130.5</td>
</tr>
</tbody>
</table>
### Physical Specifications

<table>
<thead>
<tr>
<th>Weight (full configuration)</th>
<th>10KG</th>
<th>10KG</th>
<th>22KG</th>
<th>22KG</th>
<th>24KG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant power supply</td>
<td>Standard</td>
<td>Standard</td>
<td>Standard</td>
<td>Standard</td>
<td>Standard</td>
</tr>
<tr>
<td>AC power supply</td>
<td>100~240V</td>
<td>100~240V</td>
<td>100~240V</td>
<td>100~240V</td>
<td>100~240V</td>
</tr>
<tr>
<td>DC power supply</td>
<td>-48~60V</td>
<td>-48~60V</td>
<td>-48~60V</td>
<td>-48~60V</td>
<td>-48~60V</td>
</tr>
<tr>
<td>Maximum power</td>
<td>170W</td>
<td>170W</td>
<td>350W</td>
<td>350W</td>
<td>350W</td>
</tr>
</tbody>
</table>

#### Operating environment
- Temperature: 0℃ to 40℃/5℃ to 40℃ (with optional HDD)
- Humidity: 10% to 90%

#### Non-operating environment
- Temperature: -40℃ to 70℃/Humidity: 5% to 95%

### Certifications
- ICSA Labs: Firewall, IPS
- Hardware: CB, CCC, CE-SDOC, ROHS, REACH&WEEE(EU), C-TICK, ETL, FCC&IC, VCCI, BSMI

### Functions

#### Access Control
- (Application, Time, User, Attack, Location)-based access control

#### Application Awareness
- Fine-grained identification of over 6000 application protocols, application-specific action, and online update of signature databases.

#### User Awareness
- Eight authentication methods (local, RADIUS, HWTACACS, Secure ID, AD, CA, LDAP, and Endpoint Security)

#### Intrusion prevention
- Provides over 5000 signatures for attack identification. Supports user-defined IPS signatures. Defense against web application attacks, such as cross-site scripting and SQL injection attacks.

#### Anti-Virus
- Combination of application identification and virus scanning to recognize the viruses (more than 5 millions), Trojan horses, and malware hidden in applications

#### URL Filter
- Cloud-based URL filtering with a URL category database that contains over 85 million URLs in over 130 categories; URL blacklist and whitelist and keyword filtering.

#### VPN
- VPN technologies: IPSec VPN, SSL VPN, L2TP VPN, MPLS VPN, and GRE. Support DSVPN.

#### Routing
- IPv4: static routing, RIP, OSPF, BGP, and IS-IS
- IPv6: RIPng, OSPFv3, BGP4+, IPv6 IS-IS, IPv6 RD, and ACL6

#### Security virtualization
- Virtualization of security features, forwarding statistics, users, management operations, views, and resources (such as bandwidths and sessions)

#### Anti-DDoS
- Defense against more than 10 types of DDoS attacks, such as the SYN flood and UDP flood attacks

#### Working mode and availability
- Transparent, routing, or hybrid working mode and high availability (HA), including the Active/Active and Active/Standby mode

#### Intelligent management
- Smart Policy: evaluates the network risks based on the passed traffic and intelligently generates policies based on the evaluation to automatically optimize security policies. Supports policy matching ratio analysis and the detection of conflict and redundant policies to remove them, simplifying policy management.
- Provides a global configuration view and integrated policy management. The configurations can be completed in one page.
- Provides visualized and multi-dimensional report display by user, application, content, time, traffic, threat, and URL.