



## Certifications and Testing

Industry-recognized third-party testing ensures FortiOS adheres to sound security practices while providing Unified Threat Management Services.

### NIST Validation

Since version v2.5, FortiOS firmware releases have been successfully validated against published FIPS PUB 140-2 standards.

The use of FortiOS in a FIPS approved mode of operation is a requirement of Government agencies and customers alike where assurances of data security are needed.

FIPS PUB 140-2 requirements are defined by the National Institute of Standards and Technology (NIST) – a US federal agency that develops new security standards. FIPS testing is designed to ensure that secure traffic is protected from tampering and unauthorized disclosure.

When using a FIPS-certified version of FortiOS in the FIPS-compliant mode of operation, weak cryptographic algorithms and insecure management services are disabled to ensure that traffic is protected with the strongest methods possible.

Both the FortiOS firmware and FortiASIC hardware cryptographic implementations are validated to ensure they are correctly implemented. Algorithm verification and integrity self-tests are implemented and execute when cryptographic encrypt and decrypt operations are performed to ensure that the integrity of data and the FortiGate unit are not compromised.

FIPS validated cryptographic implementations are often prerequisites for US Government sanctioned Common Criteria evaluations, where specific security functional requirements of FortiOS are further scrutinized and tested.

For further information on FIPS and FIPS validated products, refer to the following website: <http://csrc.nist.gov/groups/STM/cmvp/index.html>



### Common Criteria Assurance

Common Criteria EAL2+ and EAL4+ certifications of FortiOS have been conducted since v2.8. In the first half of 2011, EAL4+ certification was once again achieved for FortiOS v4.0 and more certifications are expected to complete in Canada and US-based labs in 2011.

Common Criteria focuses on functionality related to product security and management services. Common Criteria is an international standard (ISO/IEC 15408) which is recognized by over 20 countries world-wide. Previous certifications validated the secure management of evaluated FortiGate units and focused on Firewall, IPsec, AV, IPS, FortiGuard updates and HA security functional requirements.

Successful certifications confirm that the Target of Evaluation can be adopted by customers world-wide for use in environments where assurance of the deployed security solution is paramount.

Common Criteria evaluations in Canada are evaluated by the Communications Security Establishment Canada (CSEC) and in the United States by the National Information Assurance Partnership (NIAP).

For further information on Common Criteria and certified products, refer to the following website: <http://commoncriteriaportal.org>



## Recognized Third-Party Confidence

FortiGate Unified Threat Management solutions are subject to ongoing certification testing by multiple ICASA Labs programs. Fortinet is a member of several ICASA consortiums and testing programs.

ICASA subjects FortiOS security functionality to a variety of independent test methods to validate the Firewall, Intrusion Protection, AntiVirus and SSL implementations. These testing programs are structured to provide objective criteria that can be used to assess security implementations. Product testing focuses on secure device management, performance, logging and functionality intrinsic to the correct and reliable operation of the specifically evaluated technology.



ICASA Certification of FortiGates and FortiOS is perceived by customers as objective evidence that FortiOS the product meets their security requirements.

PCI-DSS compliance reports provided by ICASA takes this confidence one step further by providing customers with additional assurance that FortiOS can be deployed in environments to protect customer data and card holder services.

For more information on Fortinet product testing with ICASA Labs, visit <http://icsalabs.com/vendor/fortinet-inc>

## Future World-Wide Interoperability

The core IPv6 protocol implementation in FortiOS has been evaluated against the stringent requirements of the IPv6 Ready Logo Phase 2 program since FortiOS 3.0 MR7. Most recently, FortiOS 4.0 MR3 was added to the Phase 2 Approved Product list. Compliance with the Basic requirements of the USGv6 Profile also allows Federal Agencies in the United States to purchase FortiGate products and adhere to mandated procurement policies.

Completion of these third-party assessments ensures that the FortiOS' IPv6 implementation continues to be compliant with relevant RFCs and is ready to be deployed in both existing IPv6 networks and help with the transition of existing IPv4 networks to the new addressing scheme.



For more information on the IPv6 Ready Logo program, visit <http://ipv6ready.org>

## Product Confidence

External testing and validation of products is an integral part of Fortinet's product life-cycle. As new platforms and functionality are introduced, third-party labs will continue to ensure FortiGates and FortiOS adhere to evolving standards.

Other certifications and third-party testing efforts are underway to demonstrate that FortiGate solutions running FortiOS will allow customers to adapt to evolving security requirements.

For enquiries about FortiGate certifications, contact your local Sales group or visit [http://www.fortinet.com/aboutus/fortinet\\_advantages/certifications.html](http://www.fortinet.com/aboutus/fortinet_advantages/certifications.html)

