



Life of a Packet

White Paper

<i>Life of a Packet White Paper</i>	
Document Version:	Version 1
Publication Date:	9 October 2003
Description:	Describes packet flow through the FortiGate Antivirus firewall.
Product:	FortiOS v2.50

Fortinet Inc.

© Copyright 2003 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

Life of a Packet White Paper

v2.50

9 October 2003

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Table of Contents

A Day in the life of a packet.....	5
Ingress: a FortiGate interface receives a packet.....	5
The network interface and network device driver	5
The routing module	6
The VPN decryption module	7
The firewall module.....	7
The TCP layer and the application layer.....	10
Egress: a packet leaves the FortiGate unit.....	11
Traffic shaping	11
Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) ..	12
Conclusion.....	12

A Day in the life of a packet

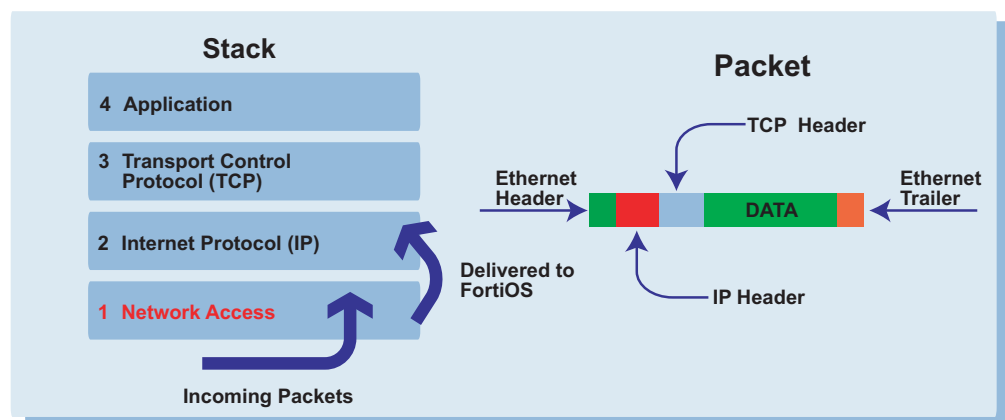
Based on Fortinet's revolutionary FortiASIC Content Processor hardware, FortiGate Antivirus Firewalls offer comprehensive multi-layer firewall protection at the network edge. Directed by firewall policies, FortiGate units screen network traffic from the IP layer up through the application layer of the TCP/IP stack.

This white paper provides a general description of what happens to a packet as it travels through the FortiGate Antivirus Firewall in both ingress (inbound) and egress (outbound) directions.

Ingress: a FortiGate interface receives a packet

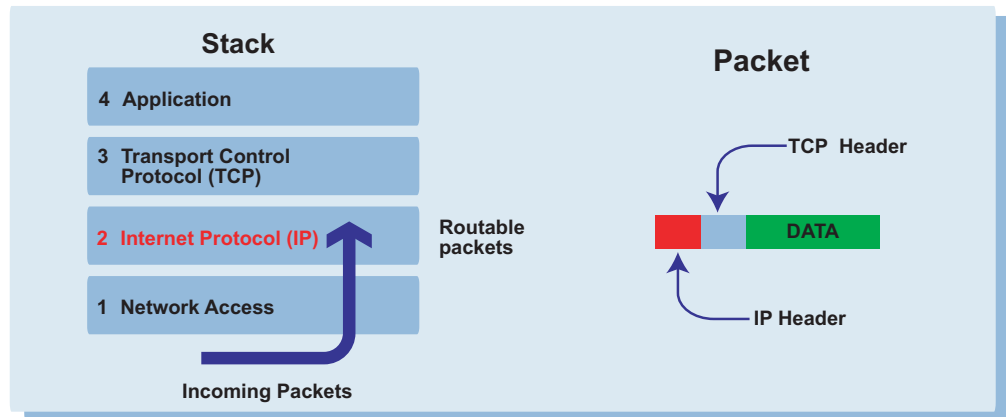
During ingress a FortiGate interface receives a packet. The interface's network device driver sends the packet to the routing module. The routing module sends the packet to the decryption module where encrypted packets are decrypted and then sent to the firewall module. The decryption module sends non-encrypted packets directly to the firewall module. The firewall module applies firewall policies to determine whether a packet is denied or accepted. If a packet contains HTTP, FTP, SMTP, POP3, or IMAP traffic and if the policy for an accepted packet includes virus scanning, web content filtering, or email filtering, the firewall module sends the packet to the application layer.

The network interface and network device driver



The first point of contact between a packet and the FortiGate unit is the network interface. Each FortiGate model has a different set of physical network interfaces. On each physical network interface, administrators can define multiple sub-interfaces. FortiGate sub-interfaces behave in almost the same way as FortiGate physical interfaces. When a FortiGate interface or sub-interface receives a packet, the network device driver selectively delivers the packet via the FortiOS to the upper layer software modules for processing.

The routing module



The FortiOS directs each packet it receives from the network device driver to the FortiGate routing module. The routing module looks at the destination address in the packet headers and decides whether or not the FortiGate unit needs to process the packet.

FortiGate units can operate in NAT/Route mode or Transparent mode. The operating mode of the FortiGate unit governs how the routing module processes packets.

NAT/Route mode routing

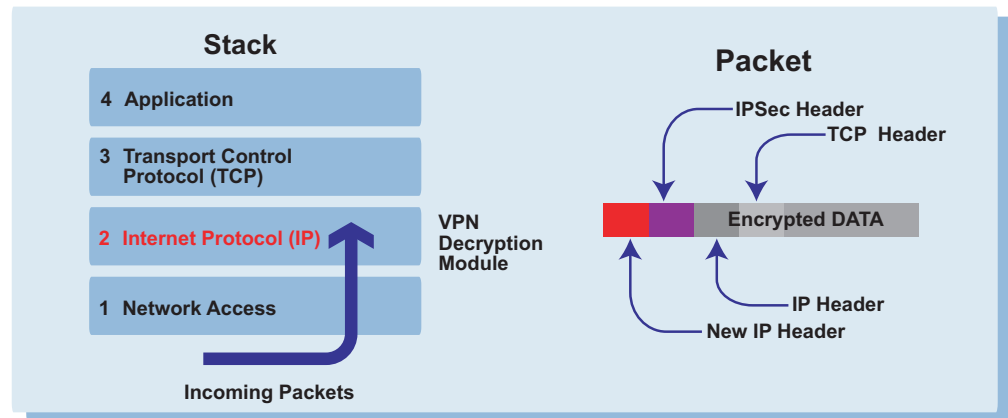
The FortiGate unit only processes packets that are sent to its layer 2 address. The FortiGate unit supports both static routing and a powerful policy routing module. Static routing routes packets based on the packet's destination IP address.

Using the policy routing module, administrators can configure routing entries based not only on the destination address in the packet header but also using any or all of, the port, the protocol number, or the source address contained in the packet header. In NAT/Route mode, FortiGate units also support the dynamic routing algorithms RIP version 1 and version 2.

Transparent mode routing

The FortiGate unit processes packets that need to be passed to another physical or administrator-defined sub-interface. If the FortiGate unit doesn't know the destination interface, it floods the packet to all interfaces except the one on which it was received.

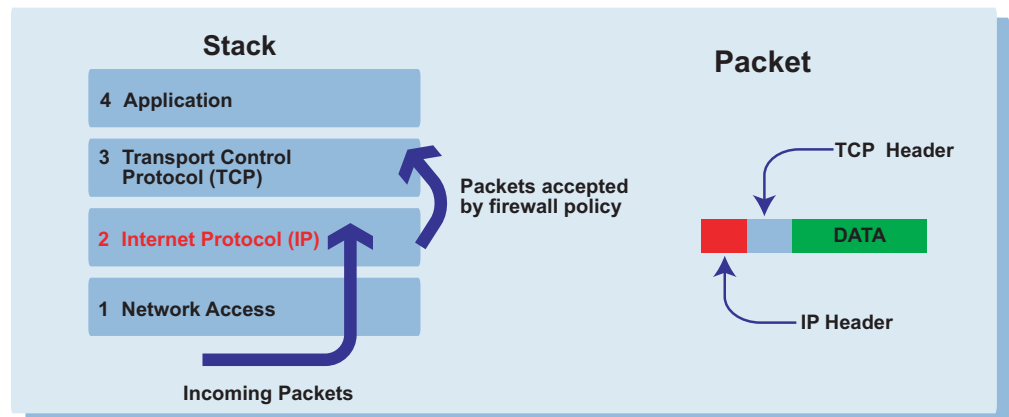
The VPN decryption module



After routing, the FortiOS sends packets to the VPN decryption module. The VPN decryption module checks whether or not the packet is encrypted. If the packet is not encrypted, the VPN decryption module sends the packet to the firewall module.

If the packet is encrypted, the VPN decryption module uses the SPI field of the packet to locate the correct VPN configuration, and then uses the correct key to decrypt the packet. The FortiASIC Content Processor accelerates decryption. After decryption, the VPN decryption module discards the external header and passes the original packet to the firewall module. If event logging is enabled, the decryption event is logged. If traffic logging is enabled, the traffic log filter will select for logging the packets and session that correspond to the decryption event.

The firewall module



All packets sent to or through the FortiGate unit must pass through the firewall module. The firewall module performs all policy enforcement and NAT functions. [Figure 1](#) shows an example policy.

Figure 1: Example policy

Policy

New Policy external -> internal

Source External_All

Destination FDS_Root

Schedule Always

Service ANY

Action ACCEPT

NAT Dynamic IP Pool
Fixed Port

Traffic Shaping Guaranteed Bandwidth (KBytes/s)
Maximum Bandwidth (KBytes/s)
Traffic Priority

Authentication RADIUS_Server02

Anti-Virus & Web filter
Content Profile

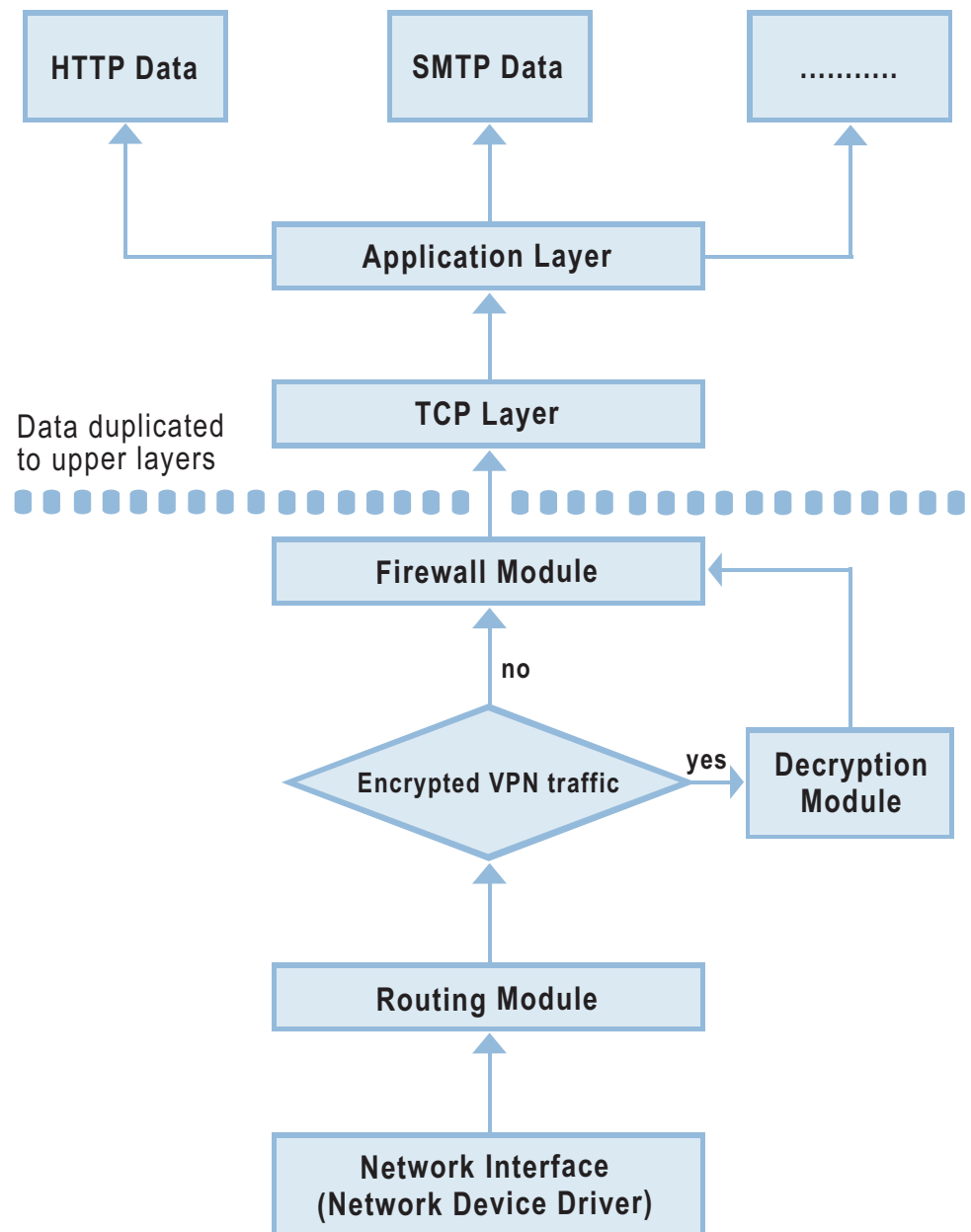
Log Traffic
Comments: maximum 63 characters

The firewall module checks the source address, destination address, and service in the packet header to see if this packet matches the policy definition.

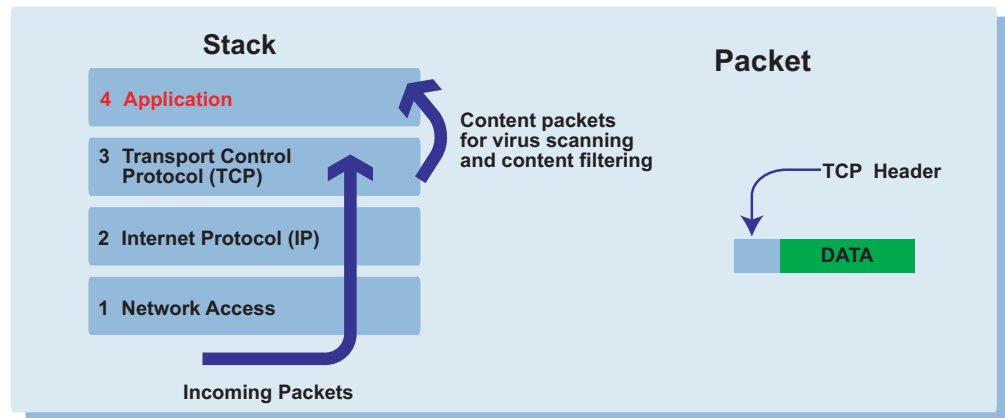
For this example policy, if the source address of a packet is a random computer on the Internet trying to connect to the FDS server and using the FDS service, the packet is allowed. Because the schedule used in this example policy is “Always”, this type of packet is always allowed. If the NAT option is checked, the firewall module replaces the source/destination IP address and TCP/UDP port numbers according to the settings specified by the user.

Packets containing the same source address, destination address, source port and destination port form a session. The first packet in a session contains the information needed for setting up the session. The firewall module keeps track of all active sessions. This means that only the first packet of the session needs to go through the full policy lookup. Subsequent packets that match the same source and destination addresses and port numbers can pass directly to the TCP layer.

Figure 2: Ingress



The TCP layer and the application layer



The firewall module checks the packets at the TCP layer. If the firewall policy associated with the packet is configured for virus scanning, web filtering, or email filtering, the firewall module sends packets accepted by this policy to the Application layer. This can include HTTP, FTP, SMTP, POP3, or IMAP packets depending on the policy settings. The FortiASIC Content Processor accelerates virus scanning, web content filtering, and email filtering.

If the policy service is set to H323, the firewall module also sends packets accepted by this policy to the Application layer.

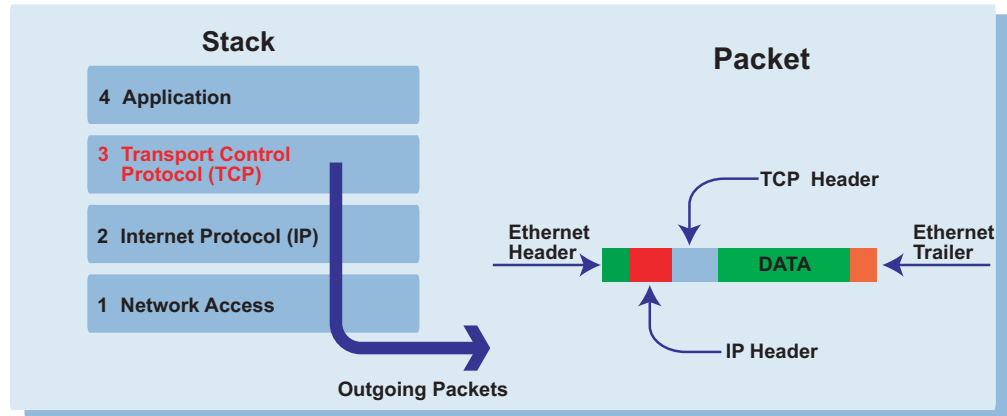
The Application layer protocols reconstruct the data. The content is then copied to a separate buffer in preparation for virus scanning, web or email content filtering, or H323 processing.

- For HTTP transfers, the Application layer protocols reconstruct URLs and web pages for web filtering, and files for antivirus file blocking and virus scanning.
- For FTP transfers, the Application layer protocols reconstruct files for antivirus blocking and virus scanning.
- For email transfers, the Application layer protocols reconstruct the entire email message, including the "From:" and "To:" fields and the content of the messages for email filtering, and attached files for antivirus file blocking and virus scanning.
- For H323 transfers, the firewall assembles H323 packets into H323 control messages and data.

Web filtering, email filtering, antivirus file blocking, virus scanning, and H323 processing all analyze the content of data once it is reassembled. The Antivirus and Web filtering modules and the firewall module use synchronization signals to keep track of the buffer status so that before the session is complete, the firewall module can take action to cancel the transfer and send an alert email. The firewall module holds onto the last few packets of a content session that is being virus scanned. If no virus is found or if the files in the session are not blocked, the FortiGate unit passes all of the remaining packets for that session and completes the transfer.

Egress: a packet leaves the FortiGate unit

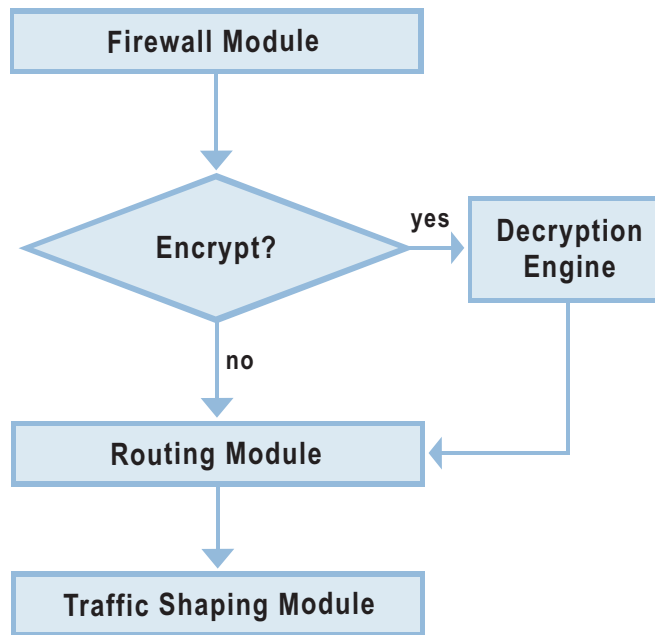
The egress path is similar to a reverse of the ingress path. After a packet leaves the firewall module, the FortiGate unit checks whether or not the packet needs to be encrypted. If the packet should be encrypted the VPN encryption module encrypts it and sends the packet to the routing module. If the packet does not require encryption, the encryption module sends it directly to the routing module. The routing module routes the packet to the appropriate network interface.



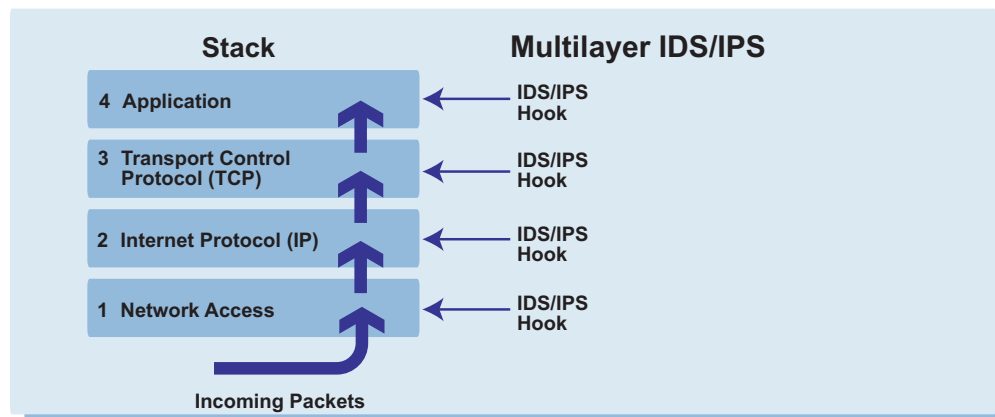
Traffic shaping

If traffic shaping is set for the policy controlling the packet, then the traffic shaping module takes action to throttle the rate at which the packets are sent according to the traffic shaping settings in the policy.

Figure 3: Egress



Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)



The FortiGate IDS/IPS feature hooks into the routing module, firewall module and Application layer. Each IDS/IPS sensor is a very lightweight traffic peeking program. The IDS/IPS sensors coordinate with the FortiASIC hardware to quickly peek into traffic and check for traffic patterns that match specified IDS signatures.

The IDS/IPS module has an additional hook into the firewall module. Once an IDS/IPS sensor identifies an attack, the firewall module quickly takes action to block the traffic so that the attack cannot complete. The firewall module will also take any additional action specified by the IDS signature, for example, blocking traffic to a specific port number from a specific source for a specified period of time. This combination of intrusion detection and prevention ensures that networks behind a FortiGate unit are protected from malicious traffic.

Conclusion

FortiGate Antivirus Firewalls provide multilayer firewalling and application level content screening. With the help of the proprietary FortiOS and the FortiASIC Content Processor, packets and sessions are screened by FortiGate units at network speeds. FortiGate units provide comprehensive security at the network edge without the delays usually associated with full content multilayer screening.