



---

# Vanguard Applications Ware IP and LAN Feature Protocols

## Firewall

# Notice

---

©2008 Vanguard Networks.  
25 Forbes Boulevard  
Foxboro, Massachusetts 02035  
Phone: (508) 964-6200  
Fax: 508-543-0237  
All rights reserved  
Printed in U.S.A.

## **Restricted Rights Notification for U.S. Government Users**

---

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

### **Restricted Rights Legend**

Use, duplication, or disclosure by the Government  
is subject to restrictions as set forth in  
subparagraph (c)(1)(ii) of the  
Rights in Technical Data and Computer Software  
clause at DFARS 252.227-7013.

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

### **Notice**

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

## Notice (continued)

---

### Proprietary Material

---

Information and software in this document are proprietary to Vanguard Networks (or its Suppliers) and without the express prior permission of an officer, may not be copied, reproduced, disclosed to others, published, or used, in whole or in part, for any purpose other than that for which it is being made available. Use of software described in this document is subject to the terms and conditions of the Software License Agreement.

This document is for information purposes only and is subject to change without notice.

Part No. T0293, Rev B  
Publication Code: TK  
First Printing: June 2009

Manual is current for Release 7.3 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to [vntechsupport@vanguardnetworks.com](mailto:vntechsupport@vanguardnetworks.com)

This page intentionally left blank.

## Firewall

Overview .....	1
Firewall Configuration .....	3
Firewall Policies .....	7
Statistics .....	12
Firewall Control-Plane, Intrazone Policies and Firewall Policy Traffic Logging	14
DoS Mitigation .....	18

This page intentionally left blank.

## Overview

### Introduction

A firewall is a set of security zones and contains a set of policies that control access between those security zones.

There are typically three types of security zones

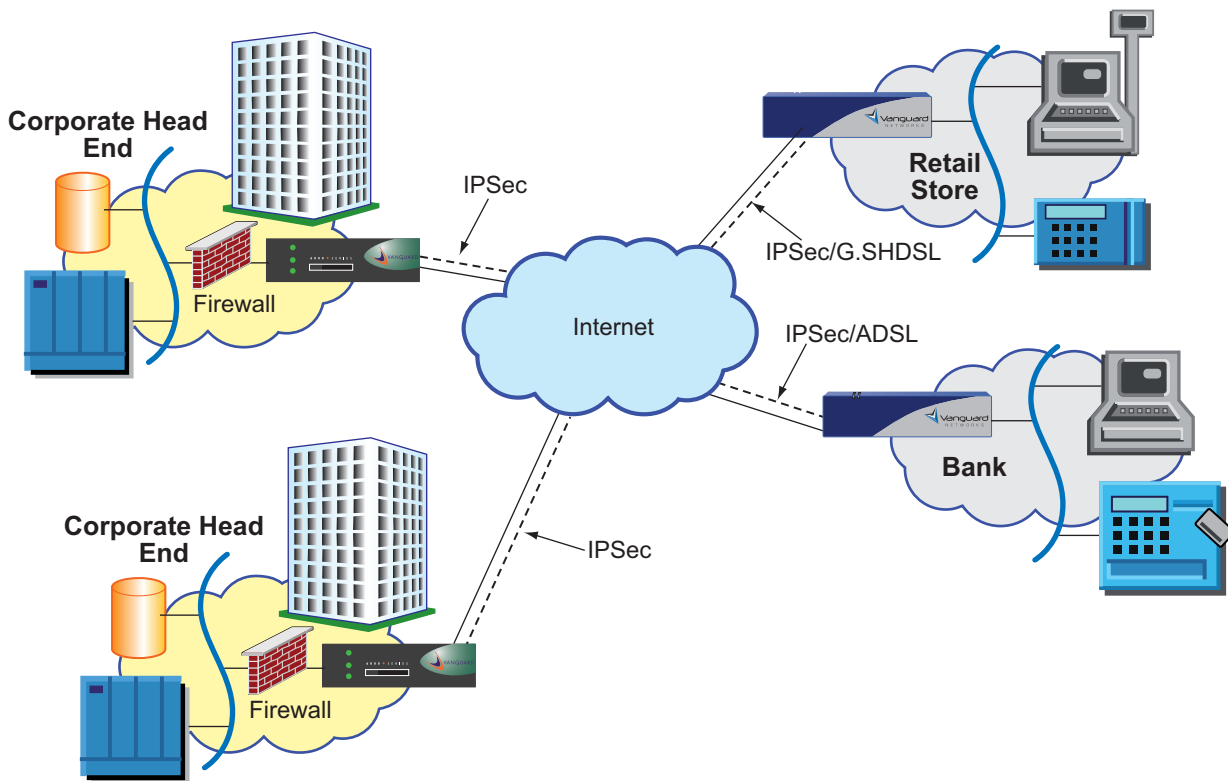
- Trust
- Untrusted
- DMZ

Vanguard Network's Firewall-DMZ feature provides an intermediate Security Zone that can be accessible from both external and internal users. DMZ provides external users controlled access to resources.

This guide explains how to configure Vanguard ports for Firewall-DMZ control.

### Application

Vanguard routers function as the hub of large enterprise networks (Figure 1) and are capable of terminating up to 1,000 encrypted tunnels plus provide an integrated stateful Firewall at the hub site. The Firewall feature can also be configured on any Vanguard router at any remote site if required.



**Figure 1. Typical Firewall-DMZ Application**

---

## Software Compatibility

Prior to release 7.2R00A Vanguard provided a limited set of firewall features. These were implemented first with “Access Control List”. However, this feature set only provided static controls and would not respond to active flow information. Firewall Lite was introduced in release 6.5R00A and provided for dynamic control via “Stateful Access Control” (for more on Firewall Lite go to page 2-133 of the Vanguard IP Routing Manual).

The new firewall feature combines the functionality of Access Control List (Static) and Stateful access control (Dynamic) to provide a more traditional firewall implementation. The new “Firewall” also introduces traditional firewall concepts, “Trusted”, “Untrusted”, and “DMZ” to the Vanguard routers and provides a cleaner configuration structure.

---

## Supported Platforms

Vanguard Networks’ Firewall-DMZ feature is included in the base IP for Release 7.2 and is supported by the following platforms.

- 68xx
- 34xx
- 73xx
- 34x

---

## Upgrading to Release 7.2R00A

When upgrading to Release 7.2R00A, you should be aware of the following:

- The new “Firewall” feature replaces the “Firewall Lite” feature and supersedes the “Access Control List” feature.
- The “Firewall Lite” feature parameters (Stateful Access Control) are replaced by Firewall and will no longer be visible to the user once a node has been upgraded to release 7.2R00A.
- If a user previously used the “Firewall Lite” feature and upgraded to 7.2R00A they **must** configure “Firewall” for the desired results.
- The access control menu and parameters will remain in the configuration and are active if the “Firewall” is disabled, but are superseded and will not function when “Firewall” is enabled. It is recommended to delete any access control list configurations if Firewall is to be utilized.

---

## About Firewall Policies

The Firewall-DMZ feature:

- Is configured between Zones, not Interfaces
  - Controls Session Creation
  - Employs an Implicit Deny at End of Policy List
  - Enables intra-zone routing if more than one interface in the zone (except Untrust)
  - Is Order Dependent
  - Allows traffic into an interface from its zone
  - Bases addresses on internal NAT addresses
-

# Firewall Configuration

---

**Introduction** This section provides a brief description of how configure the Firewall in a Vanguard Router.

---

**Configuration** The configuration of the Firewall feature in a Vanguard router includes the following:

- Enable Firewall
  - Assign Interfaces to Trust and DMZ.
  - Unassigned interfaces are Untrusted.
  - Set timeouts if needed
  - Create a list of Policies between each pair of zones.
  - Boot Global FW Parameters
  - Boot Firewall Policies
- 

**Configuring the Timeout**

When configuring the Timeout of the Firewall feature, you will be given the following options:

- Timers
  - TCP
  - UDP
  - ICMP

■ **Note**

Timers Need to be larger than expected traffic.

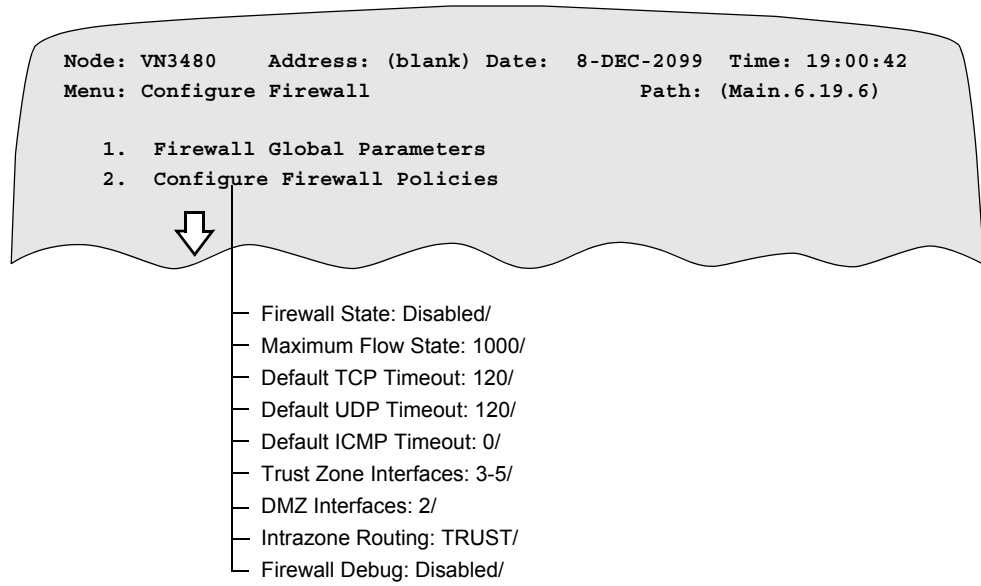
---

**Configure Firewall Record**

Figure 2 shows the location of the Configure Firewall Record and lists the parameters.

Follow these steps to configure the Firewall Record for the node.

<b>Step</b>	<b>Action</b>	<b>Result</b>
<b>1</b>	Select <b>Configure-&gt;Firewall</b> from the Main CTP menu.	The Configure Firewall menu appears as shown in Figure 2.
<b>2</b>	Select <b>Configure Firewall Policies</b> from the <b>Configure Firewall</b> menu to access the menu parameters available for configuring the SNMP Agent.	The Firewall Policies Record and its parameters appear as shown in Figure 2. A prompt appears asking you to configure the next parameter.



**Figure 2. Configure Firewall Record**

**Firewall Global Parameters**

This tables below describe the parameters that make up the Firewall Global Parameters record.

**■Note**

Unless otherwise indicated you must Boot Firewall Global Parameters for changes to these parameters to take effect.

**Firewall State**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter specifies whether the Firewall is enabled or disabled.

**Maximum Flow State**

Range	0-65535
Default	0
Description	This specifies the maximum number of flow states the router will keep. When the router has created the maximum number of flows, it will only allow new flow states to be created when the old ones are removed.

**Default TCP Timeout**

Range	10-3600
Default	120
Description	This parameter specifies whether the Firewall is enabled or disabled. This specifies the number of seconds a TCP flow state is kept (if no traffic). All protocols that use TCP (e.g., FTP) also use this timeout.

**Default UDP Timeout**

Range	10-3600
Default	120
Description	This specifies the number of seconds a UDP flow state is kept (if no traffic).

**Default ICMP Timeout**

Range	10-3600
Default	10
Description	This specifies the number of seconds an ICMP flow state is kept (if no traffic).

**Trust Zone Interfaces**

Range	1-1000
Default	
Description	This specifies the interfaces in the Trust Zone. Interfaces that are not explicitly in the Trust Zone or the DMZ are in the Untrusted Zone. A maximum of 8 ranges are permitted to be configured in this list. Ex: 1,5,7-10,20-25,31 ALL: This option puts all interfaces in the Trust Zone. NONE: This option removes all interfaces from the Trust Zone.

### DMZ Interfaces

Range	1-1000
Default	
Description	This specifies the interfaces in the DMZ. Interfaces that are not explicitly in the Trust Zone or the DMZ are in the Untrusted Zone. A maximum of 8 ranges are permitted to be configured in this list. Ex: 1,5,7-10,20-25,31 ALL: This option puts all interfaces in the DMZ. NONE: This option removes all interfaces from the DMZ.

### Intrazone Routing

Range	NONE,TRUST,DMZ,UNTRUST
Default	NONE
Description	This parameter specifies the zone(s) in which packets are routable between subnets within that zone. Any combination may be specified by summing. Ex: TRUST+DMZ

### Firewall Debugging

Range	Enabled, Disabled
Default	Disabled
Description	Enable Firewall Debug messages. This parameter is available only if Node debug is enabled.

## Firewall Policies

---

### Introduction

This section provides a brief description of the Firewall-DMZ Policies.

---

### Firewall Policies

Configuring the Vanguard router for DMZ:

- Will control traffic between Firewall Zones.
  - Will controls Session creation
  - Is based on both Ingress and Egress Zones.
  - Is order Dependent
- 

### Firewall Policy Guidelines

It is recommended when configuring your Vanguard router for Firewall Policy to adhere to the following guidelines:

- Generally permit traffic from a more secure zone to a less secure zone.
- Generally DENY traffic from a less secure zone to a more secure zone.
- Permit ONLY necessary traffic from a less secure zone to a more secure zone.
- Open the entire TCP port range when configuring for FTP support
- Open IKE and ISAMKP ports when configuring for IPSEC

■ **Note**

Policies are processing is order dependent.

---

### Firewall Policy Caveats

There are minor caveats that you should be aware of when configuring your Vanguard router for Firewall Policy. They are:

- No DoS protection
- No anti-virus support
- No ALGs
- ICMP operation

■ **Note**

From 7.3.R00A, Denial of Service (DoS) is supported by 7300, 6840, and 3400 series products.

---

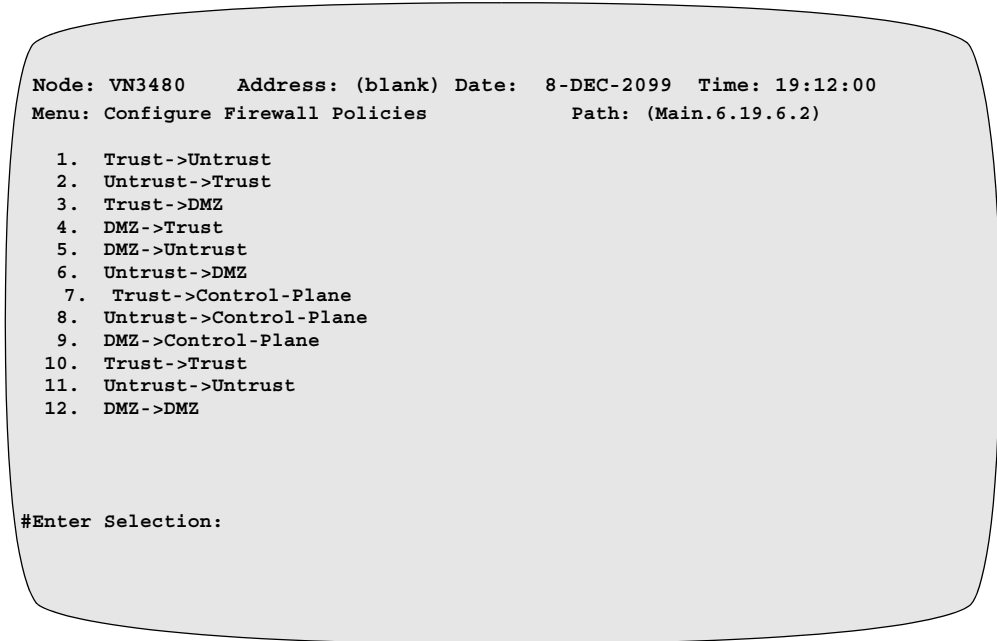
### Firewall Policy Parameters

The following parameters will be configured to enable Firewall-DMZ in a Vanguard router:

- Policy Action
- SRC/DEST addresses & Masks
- Protocols
- Port Numbers

### Configure Firewall Policies

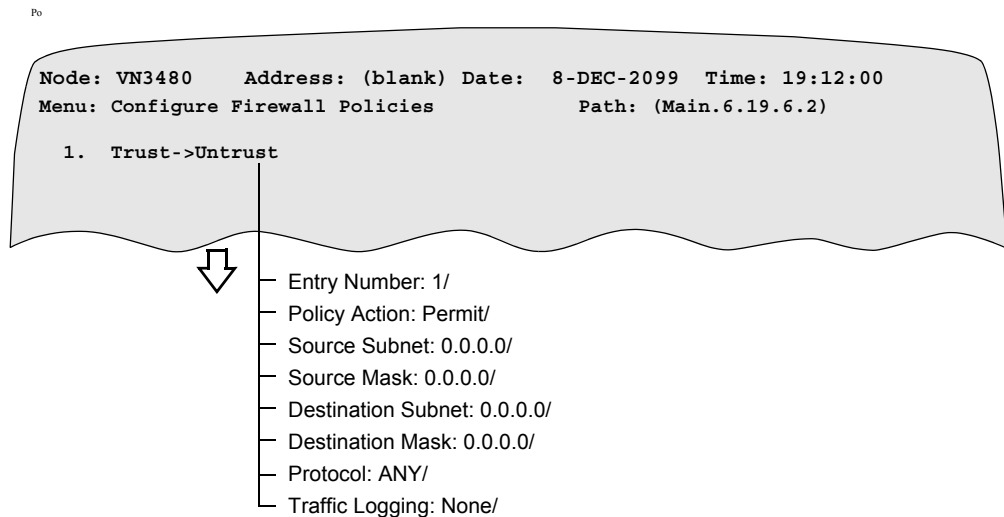
Figure 3 shows the location of the Configure Firewall Policies Record.



**Figure 3. Configure Firewall Policies Record**

### Policy Parameters

Figure 4 shows the location of all Firewall Policy records and lists the parameters. Shown as an example is the Trust->Untrust policy record.



**Figure 4. Configure Firewall Policies Trust->Untrust Parameters**

**Firewall Policies**

The tables below describe the parameters that make up the Firewall Policies Record. These parameters are applicable for each of the six policy paths available for configuration.

■ **Note**

Unless otherwise indicated you must Boot Firewall Policies for changes to these parameters to take effect.

**Entry Number**

Range	1-255
Default	1
Description	Entry number used to reference this table record.

**Policy Action**

Range	Permit, Deny
Default	Deny
Description	This parameter specifies whether the flow is permitted or denied.

**Source Subnet**

Range	A valid IP address in dotted notation
Default	0.0.0.0
Description	This parameter specifies the source subnet for this policy. It is of the form X.X.X.X.

**Source Mask**

Range	A valid IP address in dotted notation
Default	0.0.0.0
Description	This parameter specifies the source subnet mask for this policy. It is of the form X.X.X.X.

**Destination Subnet**

Range	A valid IP address in dotted notation
Default	0.0.0.0
Description	This parameter specifies the source subnet for this policy. It is of the form X.X.X.X.

### Destination Mask

Range	A valid IP address in dotted notation
Default	0.0.0.0
Description	This parameter specifies the source subnet mask for this policy. It is of the form X.X.X.X.

### Protocol

Range	Protocol number between 1-255, or TCP,UDP,ICMP or ANY
Default	ANY
Description	This parameter specifies the protocol for this policy. It can be TCP, UDP, ICMP, ANY, or a range of numbers from 1-255.

### Traffic Logging

Range	None, Start, End
Default	None
Description	This parameter controls the logging of events to the Firewall Traffic Log and to Syslog, if Syslog is enabled. None - Logging is disabled. Start - An event is logged when a flow matching this policy is created. End - An event is logged when a flow matching this policy closes. <b>■Note</b> Close events reflect the statistics for the entire session. Specify a combination by summing individual values (ex: Start+End)

**Policy Order**

Figure 5 shows the Policy Order of the Configure Firewall Policies parameters.

1	Permit	0.0.0.0/ 0.0.0.0	192.168.100.100/ 255.255.255.255	TCP	0	-65535	80 -80 443 -443
2	Permit	0.0.0.0/ 0.0.0.0	192.168.100.200/ 255.255.255.255	TCP	0	-65535	25
3	Permit	0.0.0.0/ 0.0.0.0	192.168.100.200/ 255.255.255.255	UDP	0	-65535	25
4	Permit	0.0.0.0/ 0.0.0.0	192.168.100.100/ 255.255.255.255	ICMP			
5	DENY	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	ANY			

**Figure 5. Policy Order**

## Statistics

### Viewing Firewall-DMZ Statistics

Firewall-DMZ statistics provide detailed information about Firewall Policy configuration. You can view and reset Firewall Policy statistics from the CTP for the Vanguard.

### View Statistics

Follow these steps to view the Firewall Policy Statistics menu screen.

Step	Action	Result
1	From the CTP Main Menu, select <b>Firewall Policy Stats</b> .	The Firewall Policy Statistics menu appears.
2	Select any of the six Firewall Policy Statistics as shown in Figure 6.	The selected Firewall Policies Statistics Record appears.

```

Node: VN3480   Address: (blank)           Date: 8-DEC-2099 Time: 19:20:00
Menu: Firewall Policy Stats              Path: (Main.5.16.6.1)

1. Trust->Untrust
2. Untrust->Trust
3. Trust->DMZ
4. DMZ->Trust
5. DMZ->Untrust
6. Untrust->DMZ
7. Trust->Control-Plane
8. Untrust->Control-Plane
9. DMZ->Control-Plane
10. Trust->Trust
11. Untrust->Untrust
12. DMZ->DMZ

#Enter Selection:
    
```

**Figure 6. Firewall Policy Statistics Menu**

### View Untrust->DMZ Statistics

Follow these steps to view the Untrust->DMZ Statistics menu screen.

Step	Action	Result
1	From the CTP Main Menu, select <b>Firewall Policy Stats</b> .	The Firewall Policy Statistics menu appears. Figure 2.
2	Select <b>Untrust-&gt;DMZ Stats</b> as shown in Figure 7.	The <b>Untrust-&gt;DMZ Stats</b> Record appears.

```
Node: VN3480   Address: (blank)   Date: 8-DEC-2099   Time: 19:20:44
Firewall Policies: Utrust->DMZ

A SRC Subnet/Mask   DST Subnet/Mask   Proto   SRC ports   DST ports   Count
P 150.30.1.152/32   150.30.151.128/25 1-255           12345678
D 150.30.1.0/24     150.30.151.0/25   1-255           0
D 0.0.0.0/0         0.0.0.0/0         1-255           0

Press any key to continue ( ESC to exit ) ...
```

**Figure 7. Untrust->DMZ Statistics Menu**

## Firewall Control-Plane, Intrazone Policies and Firewall Policy Traffic Logging

### Overview

Firewall Control-Plane policies control traffic destined to the firewall in the same way general firewall policies control traffic between zones across the firewall. These policies provide finer control to traffic terminating at the router itself.

And intrazone policies inside the same zone such as Trust -> Trust, Untrust -> Untrust, and DMZ -> DMZ, now enable to control traffic within the same zone.

Firewall policies will have an option to log traffic matching the firewall policy. These entries are recorded in the new Traffic Log.

### Firewall Control-Plane Policies

Firewall control plane policies are used to filter traffic terminating at the router itself. A separate set of policies is advantageous for several reasons. In many cases traffic may not need filtering through the router. In these cases, subjecting all packets to the policies is known to significantly increase the CPU utilization. By separating the policy control for traffic to the router into a separate set, it also makes the intent of the configuration much clearer.

In Configure Firewall Policies, Trust -> Control-Plane, Untrust -> Control-Plane, and DMZ -> Control-Plane are added as follows:

```
Node: Node3463 Address: 3463 Date: 24-JUN-2010 Time: 13:56:17
Menu: Configure Firewall Policies Path: (Main.6.15.6.2)

1. Trust->Untrust
2. Untrust->Trust
3. Trust->DMZ
4. DMZ->Trust
5. DMZ->Untrust
6. Untrust->DMZ
7. Trust->Control-Plane
8. Untrust->Control-Plane
9. DMZ->Control-Plane
```

**Figure 8. Configure Firewall Policies**

**Firewall Intra Zone Policies**

Firewall Intra Zone policies are used to filter traffic terminating within the same zones.

This feature is available from 7.3.R00A.

In Configure Firewall Policies, Trust -> Trust, Untrust -> Untrust, and DMZ -> DMZ are added as follows:

```
Node: Node3460 Address: 3460 Date: 28-JUL-2010 Time: 14:33:29
Menu: Firewall Policy Stats Path: (Main.5.23.8.1)

1. Trust->Untrust
2. Untrust->Trust
3. Trust->DMZ
4. DMZ->Trust
5. DMZ->Untrust
6. Untrust->DMZ
7. Trust->Control-Plane
8. Untrust->Control-Plane
9. DMZ->Control-Plane
10. Trust->Trust
11. Untrust->Untrust
12. DMZ->DMZ
```

**Figure 9. Firewall Policy Statistics**

## Firewall Policy Traffic Logging

Each firewall policy has a configurable parameter, Traffic Logging, to enable or disable logging for packets matching that policy. The default policy (implicit deny, if no policies match) has no logging. To log a catch-all deny, an explicit policy must be configured.

### Traffic Logging:

Range	None, Start, End
Default	None
Description	<p>This parameter controls the logging of events to the Firewall Traffic Log and to Syslog, if Syslog is enabled.</p> <p>None - Logging is disabled.</p> <p>Start - An event is logged when a flow matching this policy is created.</p> <p>End - An event is logged when a flow matching this policy closes.</p> <p><b>Note</b> Close events reflect the statistics for the entire session. Specify a combination by summing individual values (ex: Start+End)</p>

The traffic logging messages contain:

- Year-Month-Day
- Time (to the second)
- Action (Permit or Deny)
- Ingress Zone
- Egress Zone
- Policy Entry Number
- Source Address
- Destination Address
- Protocol
- Source Port number (if applicable)
- Destination Port number (if applicable)
- Reason

## Traffic Log Statistics

The traffic log is kept in memory as a separate log for viewing by the operator. For ease of searching, it shall be kept as an array of traffic log data structures. The array size should be 4K entries.

An entry will be added under the existing Firewall Stats menu, "Firewall Traffic Log". Select "Firewall Traffic Log" to view the current entries in the traffic log.

```
Node: root Address: (blank) Date: 21-NOV-2000 Time: 22:48:47
Menu: Firewall Stats Path: (Main.5.16.6)

1. Firewall Policy Stats
2. Firewall Traffic Log

#Enter Selection: 2
↓
Node: root Address: (blank) Date: 21-NOV-2000 Time: 22:48:47
Firewall Traffic Log Page: 1

start_time="2003-04-19 02:00:55" ingress_zone=DMZ egress_zone=Control-Plane
policy_num=2 policy_action=Permit src=172.16.1.57 dst=150.30.1.74 proto=1
icmp_type=8 icmp_code=512 reason=Creation
```

Figure 10. Traffic Log Statistics

## DoS Mitigation

### Overview

---

From 7.3.R00A, Vanguard Router can eliminate Denial of Service (DoS) attacks such as bad packets, bad TCO flags, and fake requests to enhance network security and ensure PCI DSS (Payment Card Industry Data Security Standard) compliance. Under the “Configure Firewall” menu, a ”Configure DoS Mitigation” selection is added. DoS Mitigation is configurable on a per zone basis. The zone is the one from which the traffic will originate.

---

### DoS Mitigation Configuration

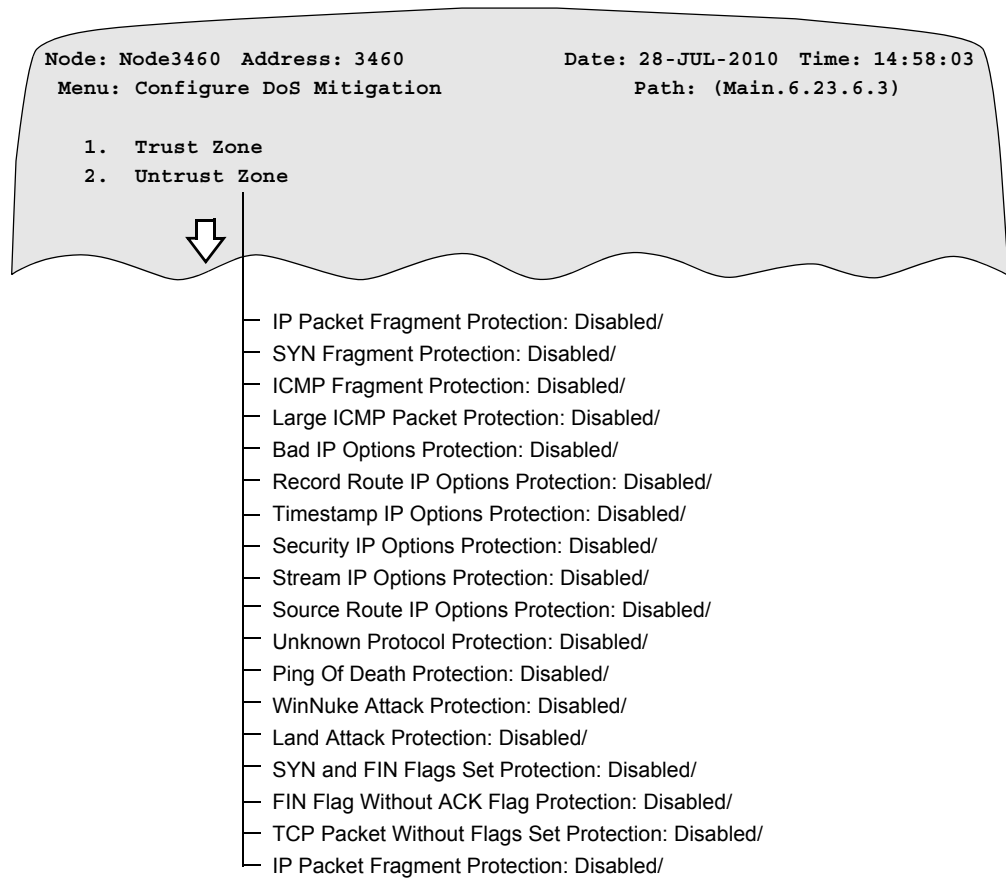
Figure 11 shows the Configure Firewall menu and Figure 12 shows the Configure DoS Mitigation menu. The tables that follow describe the Configure DoS Mitigation parameters.

```
Node: Node3460 Address: 3460 Date: 28-JUL-2010 Time: 14:56:07
Menu: Configure Firewall Path: (Main.6.23.6)

1. Firewall Global Parameters
2. Configure Firewall Policies
3. Configure DoS Mitigation

#Enter Selection: 3
```

**Figure 11. Configure Firewall Menu**



**Figure 12. Configure DoS Mitigation Menu**

### IP Packet Fragment Protection

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of fragmented IP packets. If enabled, a packet is discarded if the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

### SYN Fragment Protection

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of fragmented TCP SYN packets. If enabled, a packet is discarded if the SYN flag is set, and the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

**ICMP Fragment Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of fragmented ICMP packets. If enabled, a packet is discarded if the protocol is ICMP and the More Fragments flag is set or the Fragment Offset field in the IP header is nonzero.

**Large ICMP Packet Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of large ICMP packets. If enabled, a packet is discarded if the protocol is ICMP and the total packet length field in the IP header is greater than 1024 bytes.

**Bad IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets having an invalid IP options field in the IP packet header.

**Record Route IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with the Record Route IP options bit set in the IP packet header.

**Timestamp IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with the Timestamp IP options bit set in the IP packet header.

**Security IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with the Security IP options bit set in the IP packet header.

**Stream IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with the Stream IP options bit set in the IP packet header.

**Source Route IP Options Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with the Loose Source Route or the Strict Source Route IP options bit set in the IP packet header.

**Unknown Protocol Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of IP packets with an unknown protocol value in the IP packet header. If enabled, a packet is discarded if the protocol value is 143 or greater.

**Ping Of Death Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of oversized ICMP packets. If enabled, a packet is discarded if the total packet size is greater than 65,535 bytes, even if the packet is fragmented.

**WinNuke Attack Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of TCP packets having a destination port of 139 and the Urgent flag set in the TCP header. This introduces a NetBIOS fragment overlap causing many Windows machines to crash.

**Land Attack Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of TCP packets having the SYN bit set with both the source and destination IP addresses the same in the IP packet header.

**SYN and FIN Flags Set Protection: Disabled**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of TCP packets having both the SYN and FIN flags set in the TCP packet header. This is an illegal TCP flags combination.

**FIN Flag Without ACK Flag Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of TCP packets having the FIN flag set without the ACK flag set in the TCP packet header. This is an illegal TCP flags combination.

**TCP Packet Without Flags Set Protection**

Range	Enabled, Disabled
Default	Disabled
Description	This parameter controls the discarding of TCP packets having no flags set in the TCP packet header. This is an illegal TCP flags value.

## A

About Firewall Policies [1-2](#)

Application  
Firewall-DMZ [1-1](#)

## C

Caveats

Firewall Policies [1-7](#)

Configuration

Firewall Configuration [1-3](#)

Configure

Firewall Policies [1-8](#)

Configuring Firewall Record [1-3](#)

Configuring the Timeout [1-3](#)

Control-Plane Policies [1-14](#)

## D

DoS Mitigation Menu [1-19](#)

## F

Firewall Configuration [1-3](#)

Configuration [1-3](#)

Configuring Firewall Record [1-3](#)

Configuring the Timeout [1-3](#)

Firewall Global Parameters [1-4](#)

Introduction [1-3](#)

Firewall Control-Plane, Intrazone Policies and Firewall Policy Traffic Logging [1-14](#)

Firewall Global Parameters [1-4](#)

Firewall Policies [1-7](#), [1-9](#)

Caveats [1-7](#)

Configure [1-8](#)

Configuring Vanguard Router [1-7](#)

Guidelines [1-7](#)

Introduction [1-4](#), [1-7](#)

Parameters [1-7](#)

Policy Parameters [1-8](#)

Firewall-DMZ

About Firewall Policies [1-2](#)

Application [1-1](#)

Introduction [1-1](#)

Overview [1-1](#)

Software Compatibility [1-2](#)

Supported Platforms [1-2](#)

Upgrading to Release 7.2R00A [1-2](#)

## G

Guidelines

Firewall Policies  
[1-7](#)

## I

Intra Zone Policies [1-15](#)

Introduction

Firewall Configuration [1-3](#)

Firewall Policies [1-4](#), [1-7](#)

Firewall-DMZ [1-1](#)

## P

Parameters

Firewall Policies [1-7](#)

Policy Order [1-11](#)

Policy Parameters

Firewall Policies [1-8](#)

Policy Traffic Logging [1-16](#)

## S

Software Compatibility [1-2](#)

Statistics [1-12](#)

Untrust->DMZ [1-12](#)

Viewing [1-12](#)

Supported Platforms [1-2](#)

## U

Untrust->DMZ Statistics Viewing [1-12](#)

Upgrading to Release 7.2R00A [1-2](#)

## V

Viewing Firewall-DMZ Statistics [1-12](#)