



WHITE PAPER  
Deploying Network VirusWall in a  
Cisco Switched Environment

June 2004

TREND MICRO, INC.  
10101 N. DE ANZA BLVD.  
CUPERTINO, CA 95014  
T 800.228.5651/408.257.1500  
F 408.257.2003  
WWW.TRENDMICRO.COM

# Deploying Network VirusWall in a Cisco Switched Environment

## TABLE OF CONTENTS

3	Abstract
4	Introduction
4	Audience
4	Objective
4	Overview
5	Designs
5	Designs Using 802.1q Trunk
6	Single and Dual Switch Designs

June 2004  
Trend Micro, Inc.

©2003 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, AppleTrap, Control Manager, eManager, GateLock, InterScan, HouseCall, InterScan VirusWall, MacroTrap, NeaTSuite, OfficeScan, PC-cillin, PortalProtect, ScanMail, ScriptClean, ScriptTrap, ServerProtect, SmartScan, TMCM, Trend Micro Content Scanning Protocol, Trend Micro Control Manager, Trend Micro CSP, Trend Micro Damage Cleanup Server, Trend Micro Damage Cleanup Services, Trend Micro Outbreak Prevention Services, TrendLabs, Trend VCS, VirusWall, WebManager, WebProtect and WebTrap are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

## **ABSTRACT**

Trend Micro™ Network VirusWall™ is an outbreak prevention appliance that helps organizations stop network viruses (Internet worms), block high threat vulnerabilities during outbreaks, and quarantine and clean-up infection sources including unprotected devices as they enter the network, using threat-specific knowledge from Trend Micro deployed at the network layer. Unlike security solutions that only monitor threats or provide threat information, Network VirusWall helps organizations take precise outbreak security actions and proactively detect, prevent, contain, and eliminate outbreaks. By deploying Network VirusWall in network LAN segments, organizations can significantly reduce their security risk, network downtime, and outbreak management burden.

This document describes how Network VirusWall may be deployed in an infrastructure that uses Cisco switches.

## INTRODUCTION

Network VirusWall is designed as an inline device that functions as a security bridge. Therefore, it must operate within a logical LAN (VLAN) inside a Cisco switched environment. The designs that are described in this paper use basic functionalities that are available in most of the Cisco Catalyst switches.

The solution configurations in this document are based on Cisco IOS software, but most of the concepts are equally applicable to Cisco Catalyst native OS.

### Audience

This document is for network design engineers, network architects, and network support engineers who are responsible for planning, designing, implementing, and operating networks. This document is also for security professionals who are responsible for implementing security solutions in networks.

### Objective

The purpose of this document is to illustrate how to deploy an inline inspection engine into the Cisco Catalyst family of switches.

## OVERVIEW

The Network Intrusion Detection Systems (NIDS) that Cisco currently delivers (i.e., Cisco IDS 4200 series) are promiscuous listening devices designed so as to not interfere with monitored packet flows. They are essentially passive surveillance devices that can interact, at given points in time, with packet flows. This interaction could be to block the flow by introducing a Router Access Control List (RACL) on a router somewhere along the packet flow or to break off TCP connections by sending TCP resets to both sending and receiving devices.

The only requirement of the infrastructure is for the NIDS device to be able to listen to the traffic within the infrastructure. If a network hub is used then this is automatically provided based on the fact that each port on a hub contains exactly the same traffic, i.e. there is no optimization performed, and all ports are in the same collision domain. Thus with a network hub, all sessions will be monitored in a bi-directional fashion.

When a switch is introduced, the ports are no longer in the same collision domain and various optimizations are performed so only relevant traffic will be presented to each switch port. As such, only traffic directly addressed for a device on a particular port, broadcast traffic, and relevant multicast traffic is in that group. For deployment compatibility of Cisco NIDS devices in a switched environment, the usage of SPAN,

RSPAN and VACL capture provide a way to generate copies of packets flowing within a VLAN, or on given switch ports. It is important to note that copies are generated and therefore there is no impact on the original traffic flows.

The copied traffic is redirected to the NIDS via switch ports that may be on either a local or a remote switch, where the NIDS device is attached.

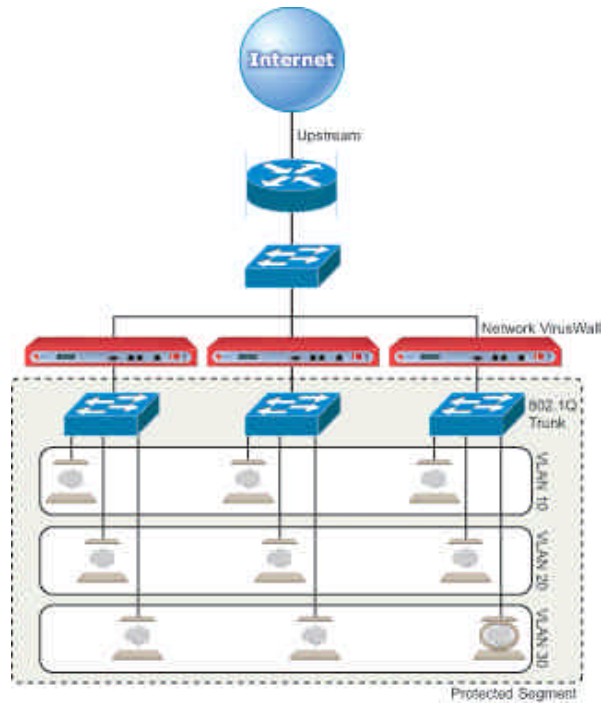
Since Network VirusWall is designed to operate in an 'inline mode' such that it sits directly in the packet path, the traditional "copy and listen" methods described above cannot be used without negatively affecting network performance and throughput. As such, we propose three means of integrating Network VirusWall into a Cisco switched environment.

## **DESIGNS**

As Network VirusWall must always be present within the packet stream to discover a virus or worm outbreak, the following section lists three designs that accomplish this within a Cisco switched environment.

### **Design using 802.1q trunk**

This design is a Dual Switch Deployment that allows traffic traversing between the two switches to be inspected on the uplinks between the switches. The uplink between the two switches is a trunk link (802.1q), in this case a fast Ethernet connection. When Network VirusWall sits on a trunk link, it is capable of inspecting multiple VLANs that are traversing that link. The only consideration that has to be taken into account is that traffic on the trunk link will be throttled to the capacity of the Network VirusWall deployed.



**Figure 1.** This is a dual switch design, where access devices are placed on vlans 10,20, and 30. The upstream router is placed on vlans 10,20, and 30. Network VirusWall is placed with a LAN interface in both on the trunk between the two switches, which allows it to monitor multiple VLANs at the same time; bandwidth restrictions will apply.

## Single and dual switch designs

In this design, vlan 20 and vlan 200 are used to enable the designs to operate within a single L2 switch.

This design is a single or dual switch deployment that allows traffic traversing between the two switches to be inspected on the uplinks between the switches. The uplink between the two switches or access ports is a general access link, in this case a Fast Ethernet connection. When the Network VirusWall sits on an access link within a VLAN, it is NOT capable of inspecting traffic on other VLANs. With this network architecture, multiple Network VirusWall devices are required to inspect multiple VLANs. The other consideration that has to be taken into account is that traffic on the uplink will be throttled to the capacity of Network VirusWall, but it is possible to scale this to a higher bandwidth through load balancing mechanisms.

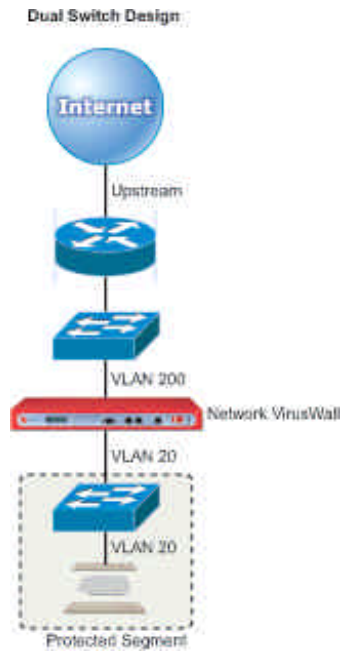


Figure 2. This is a dual switch design, where access devices are placed on vlan 20. The upstream router is placed on vlan 200. Network VirusWall is placed with a LAN interface in both vlan 20 and vlan 200, which is used to force traffic on vlan 20 to traverse Network VirusWall to reach the upstream router in vlan 200.

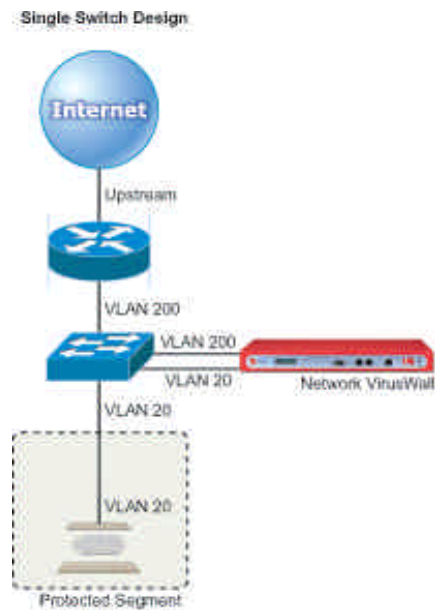
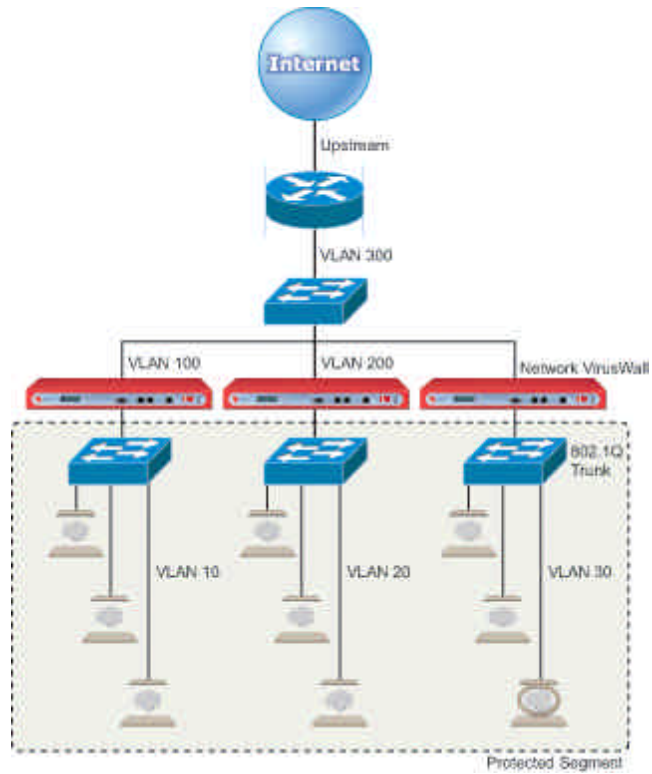


Figure 3. This is a single switch design, where access devices are placed on vlan 20. The upstream router is placed on vlan 200. Network VirusWall is placed with a LAN interface in both vlan 20 and vlan 200, which is used to force traffic on vlan 20 to traverse Network VirusWall to reach the upstream router in vlan 200.



**Figure 4.** This is a variant of the single switch design that extends the design to multiple switches and aggregates traffic into a single upstream switch and router.

## **About Trend Micro**

Trend Micro, Inc. is a leader in network antivirus and Internet content security software and services. The Tokyo-based corporation has business units worldwide. Trend Micro products are sold through corporate and value-added resellers and managed service providers. For additional information and evaluation copies of all Trend Micro products, visit our Web site, [www.trendmicro.com](http://www.trendmicro.com)