

# Compatible Systems Tech Notes: IntraGuard Bridging vs Routing and Dynamic Firewall Paths

Document ID: 17671

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Contents – Knowledge Base Article C000260

Bridging

Routing

Dynamic Firewall Paths

ORFilterIn

ANDFilterIn

### Related Information

---

## Introduction

This document explains how the Dynamic Firewall Paths work on the IntraGuard Firewall.

**Note:** All versions of IntraGuard are affected.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on the Cisco Compatible IntraGuard Firewall Series.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Contents – Knowledge Base Article C000260

### Bridging

When a port is set for bridging, it means that it does *not* look at the IP address of the packet. Bridges are not concerned about IP addresses. This is how the IntraGuard is considered a drop in firewall. In the bridged configuration right out of the box, you can put it in between your Internet router and network hub without the

need to assign it an IP address from your network. But, in order to access it with Compatiview or Telnet, you need to assign it an IP address from your network.

Bridged ports pass broadcast traffic across to any other bridged port and create a table of the MAC addresses it knows for each port. If it knows that the MAC address of the packet is on a particular port, then it sends it directly to that port. Otherwise, it sends that packet out every other bridged port.

## Routing

When a port is set for routing, it means that it looks at the IP address of the packet. If it knows where the IP destination network is, then it routes it out to the proper port in order to reach that destination. The routed port does not pass broadcast traffic. This is why software such as Microsoft Networking, which depends heavily on broadcast traffic and the non-routable protocol netbeui, does not work when two networks are separated by a router.

**Note:** Routers route between different IP networks or subnets.

## Dynamic Firewall Paths

The high speed firewalling capability of IntraGuard depends on Firewall Paths. Firewall Paths are *bridged* paths between these two interfaces:

- InsideInterface
- OutsideInterface

The IntraGuard only filters traffic along these paths. Any port on the IntraGuard set to routing is not able to utilize a Firewall Path and its dynamic filtering capabilities.

For instance, the default Green-Red path has this setup:

```
SecurityPolicy      =      Standard
  OutsideInterfaces =      Ether 2
  InsideInterfaces  =      Ether 0
  InsideInterfaces  =      Bridge
```

In this setup, Ethernet 0 and Ethernet 2 are bridged. Any traffic that passes between them flows across the Green-Red path because this path has an OutsideInterface of Ethernet 2 and an Inside Interface of Ethernet 0. So the Standard Security Policy are applied to any traffic that use this Dynamic Firewall Path.

If Ethernet 0 and Ethernet 2 were changed to *routed*, then there is no traffic bridged between them. Without bridging, the Dynamic Firewall is not applied to traffic passing between Ethernet 2 and Ethernet 0.

In the recommended NAT configuration for the IntraGuard, Ethernet 0 is routed and Ethernet 2 is Bridged, and the Green-Red Path looks like this:

```
SecurityPolicy      =      Standard
  OutsideInterfaces =      Ether 2
  InsideInterfaces  =      Bridge
```

This is how the Dynamic Firewall Path applies. In order for traffic to go from Ethernet 2 to Ethernet 0, it must first be bridged to the Bridge port, NATted, and then routed to the Ethernet 0 port. The Green-Red Security Policy is applied to the traffic when it is bridged from OutsideInterface Ethernet 2 to InsideInterface Bridge. Then, if the traffic makes it through the Security Policy, the destination address is translated with the use of NAT, and routed on to its destination out Ethernet 0 to the private network.

The same theory and configuration is used for the Green–Yellow and Yellow–Red Paths. Note that in the recommended NAT configuration, traffic that flows along the Yellow–Red Path is bridged and never gets NATted.

## ORFilterIn

This is a filter that is applied to the InsideInterface of a Dynamic Firewall Path. It creates a logical OR between the designated filter and the Security Policy of that Firewall Path. So if the Security Policy OR the Filter allows the traffic through, then it passes safely. This means that only one has to allow the traffic in order for it to pass. ORFilterIn is used in order to allow specific traffic across a Firewall Path. Do *not* use a permit 0.0.0.0 0.0.0.0 at the end of this filter or it allows all traffic through the firewall. This is an example of the filter:

```
# Allow all access to this one internal web server
  permit 0.0.0.0 204.144.171.10 tcp dst = 80
```

## ANDFilterIn

This is a filter that is applied to the InsideInterface of a Dynamic Firewall Path. It creates a logical AND between the designated filter and the Security Policy of that Firewall Path. If the Security Policy and the Filter allows the traffic through, then it passes safely. This means that both have to allow the traffic or it does not pass. ANDFilterIn is used in order to deny specific traffic across a Firewall Path. You *must* use a permit 0.0.0.0 0.0.0.0 at the end of this filter or it does not allow any other traffic through the firewall. This is an example of the filter:

```
# Deny all access to this internal web server
  deny 0.0.0.0 204.144.171.10 tcp dst = 80
  # Allow all other traffic that makes it through the Security Policy
  permit 0.0.0.0 0.0.0.0
```

---

## Related Information

- [Cisco Compatible IntraGuard Firewall Series](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Aug 23, 2007

Document ID: 17671

---