

Use WatchGuard Application Control with Your Existing Firewall

Example configuration files created with — WSM v11.4.2

Revised — 8/8/2011

Use Case

An organization wants to block the use of specific applications on their network, but they do not want to change their existing firewall configuration or any of their existing network addresses. Initially, they want to block access to all online games, and block access to Facebook.

Note *This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.*

Solution Overview

This organization can add a WatchGuard XTM device behind any firewall on their existing network to monitor and control which applications their users can use. To do this, they configure their XTM device in bridge mode, so it can transparently monitor and control content in and out of their network without any change to their existing firewall configuration or network addressing.

After the XTM device is added to the network, NAT and network routing are still managed by the existing gateways and routers. The XTM device simply examines the content as it passes through, and then applies policies to that traffic.

How It Works

In bridge mode, the XTM device does not route network traffic. The XTM device examines the traffic and then passes it on to the destination, without any changes to the packet header or routing information. When the packet arrives at a gateway from the XTM device, it appears to have been sent from the original device.

The traffic that passes through the XTM device is managed by the policies you add to the device configuration file. When Application Control is enabled in the policies, traffic is inspected to identify applications and block the traffic for the applications that you specify.

Requirements

- **An XTM device appropriate for your network size**

XTM device capabilities vary by model. You must select an XTM device that has the capacity to manage the traffic for your network. For information about XTM devices, see <http://www.watchguard.com/products/xtm-main.asp>.

- **Fireware XTM OS v11.4 or later**

To use Application Control, the XTM device must use Fireware XTM OS v11.4 or higher.

- **A security subscription to Application Control**

The XTM device must have an active Application Control security subscription.

Configuration Example

To illustrate this type of configuration, we present an example of an existing firewall that protects a private network. Because routing is managed by the existing network devices, the network behind the firewall can either be a single network or multiple subnets behind a router. The XTM device can apply Application Control rules to the traffic between the network users and the existing firewall, regardless of your network configuration.

In this configuration example, the existing network uses these IP addresses:

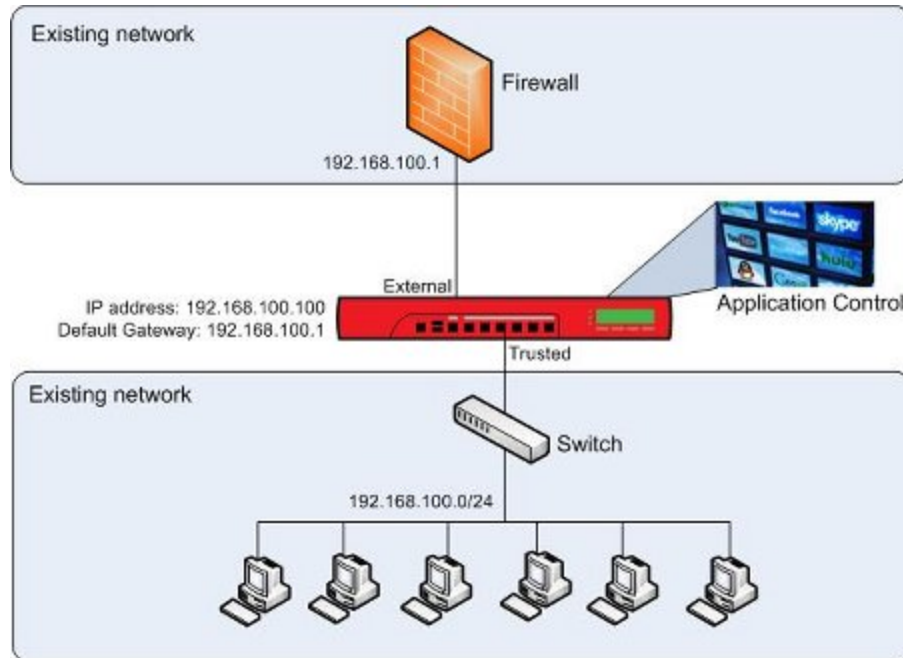
Example network configuration	IP address
Existing firewall	192.168.100.1
Private network immediately behind the existing firewall	192.168.100.0/24

To configure the XTM device, you only need to know the existing firewall IP address and an available IP address on the internal network that you can assign to the XTM device for management. As long as the XTM device is located between the network users and the firewall, the rest of the existing network topology does not affect the XTM device configuration.

To emphasize this point, we provide two different existing network topologies: Flat Internal Network and Routed Internal Network. The same XTM device configuration file can be used for either topology.

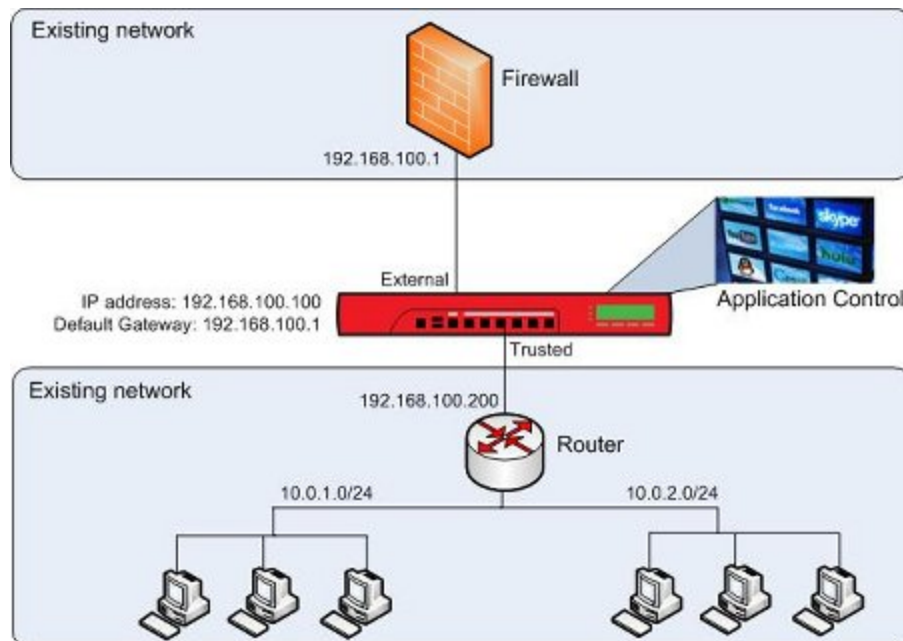
Topology 1 — Flat Internal Network

This diagram shows where to install your XTM device on a network with a single subnet, so that you can use Application Control.



Topology 2 — Routed Internal Network

This diagram shows where to install your XTM device on a network with a router and multiple subnets, so that you can use Application Control.



Example Configuration File

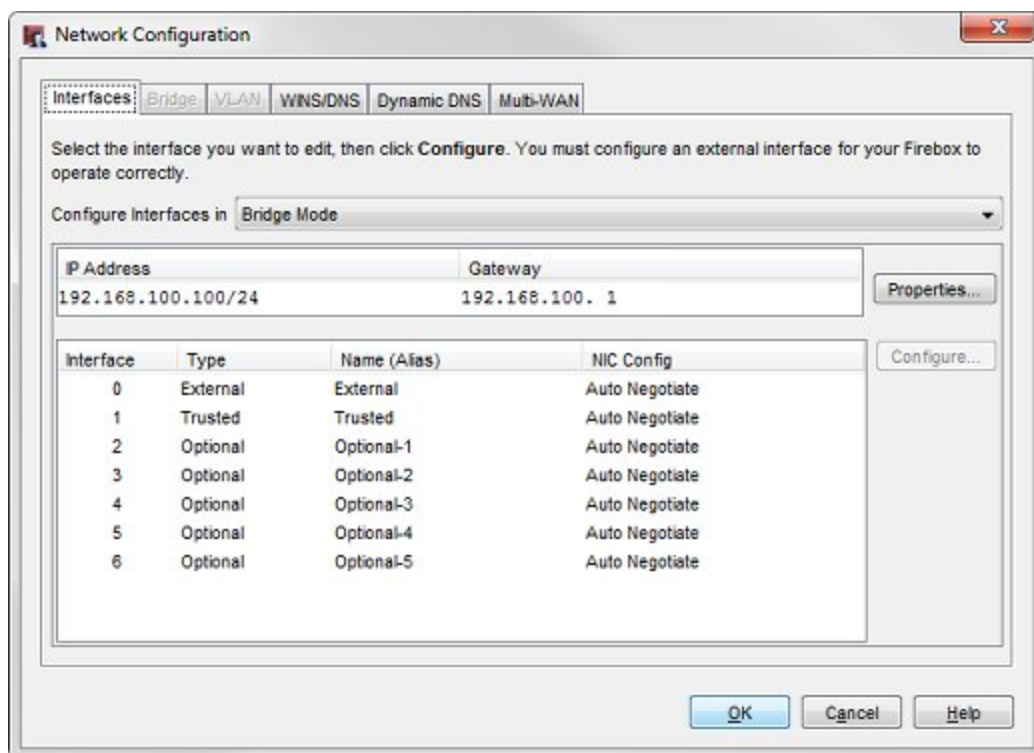
For your reference, we have included an example configuration file with this document. This example configuration file supports both of the network topologies described in the previous section. To examine the details of the example configuration file, open it with Policy Manager v11.4 or later. Application Control is not available in earlier versions of Policy Manager.

The name of the example configuration file is `app_control_bridge.xml`.

Configuration File Explained

Network Configuration in Bridge Mode

In this example configuration file, the network is configured in Bridge Mode.



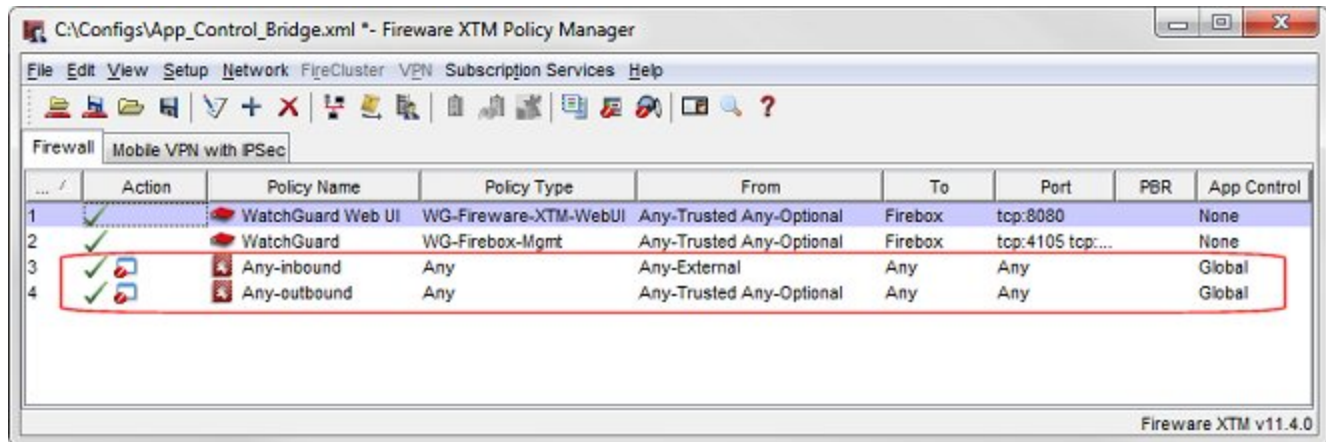
To connect to the device to manage it, you use the IP address of the XTM device. That address must be on the same subnet as the firewall. In this example, the XTM device IP address is set to 192.168.100.100/24.

The existing firewall is the default gateway for the network that is immediately behind the firewall, so the gateway IP address in the XTM device configuration file is set to the firewall IP address, 192.168.100.1.

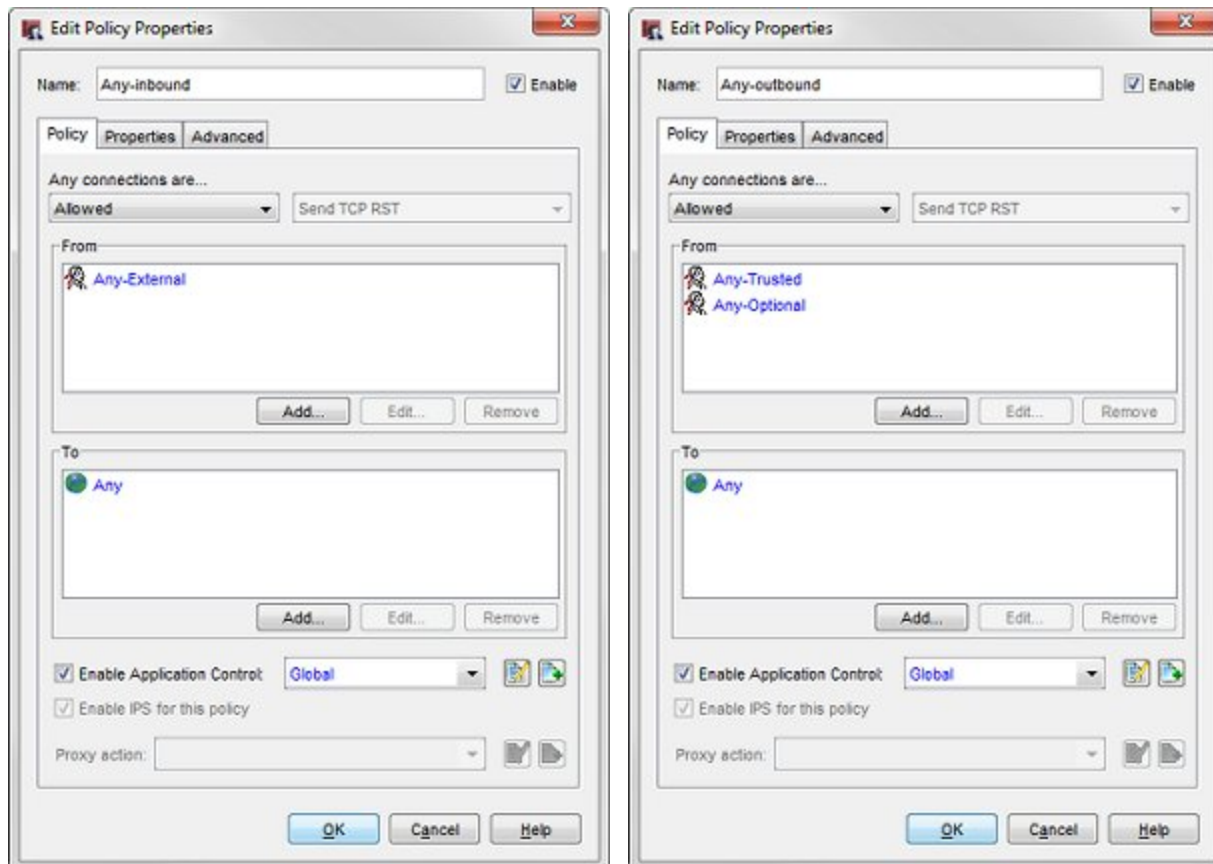
Policies

The example configuration file includes these two policies, which allow all traffic to flow through the device:

- **Any-inbound** — Allows all traffic from the firewall to the users on the network.
- **Any-outbound** — Allows all traffic from the users on the private network to the firewall.



Policies of the type *Any* apply to any type of traffic. You can double-click each of these policies to examine the policy configuration details.



Each policy has the **Global** Application Control action enabled.

Application Control Settings

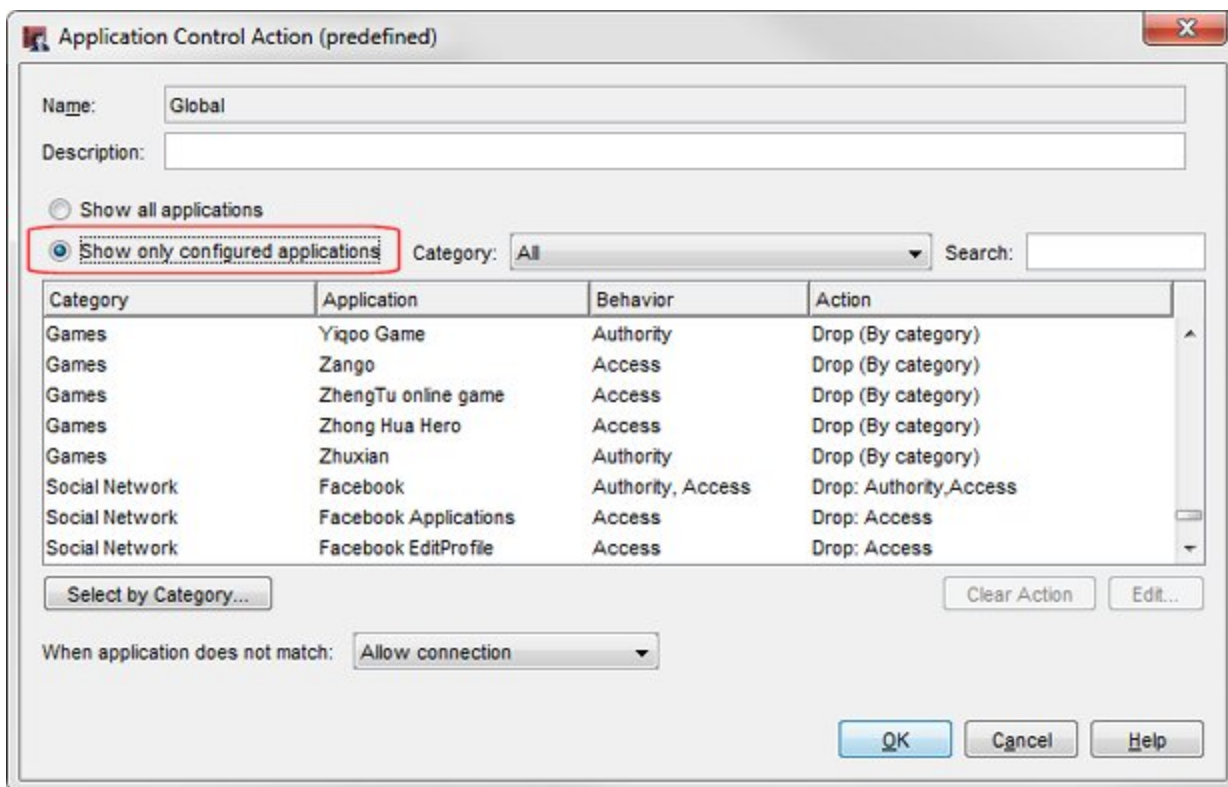
In this example configuration, the *Global* Application Control action is configured to block:

- All Facebook applications
- All applications in the Games category

This Global Application Control action is enabled for the **Any-inbound** and **Any-outbound** policies that allow the traffic.

To see the *Global* Application Control action in the example configuration file:

1. Select **Subscription Services > Application Control**.
The Application Control Actions dialog box appears.
2. From the **Actions** list, select the **Global** Application Control action and click **Edit**.
The Application Control Action (predefined) dialog box appears.
3. Select **Show only configured applications**.



In this example, all games applications are blocked based on the application category, as indicated by the selected action: **Drop (By category)**. The Facebook applications, however, are blocked individually, as indicated by the specified drop actions.

- To see which application categories are blocked, click **Select by Category**.
For this example, you can see the action for the Games category is set to Drop.



The Games category blocks all online games, not just Facebook games. This is what we want for this use case.

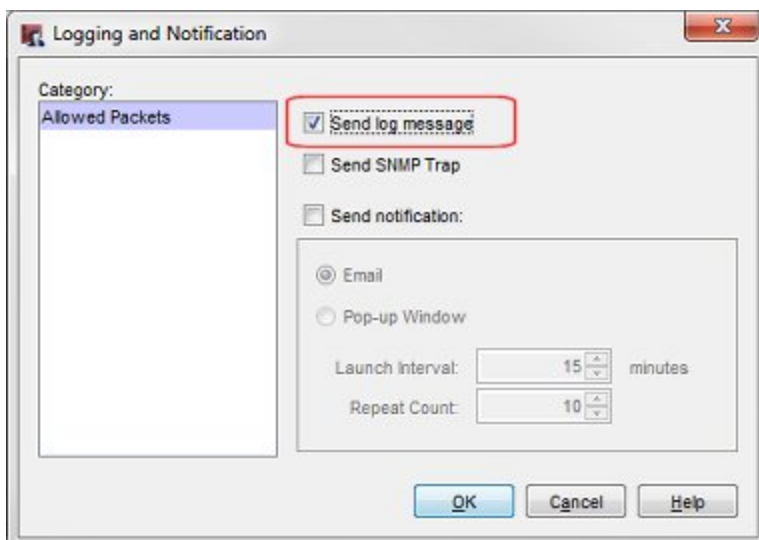
Monitor Blocked Applications

When Application Control drops traffic that matches a configured Application Control action, that event appears in a traffic log message. If you connect to the XTM device with Firebox System Manager, you can select the **Traffic Monitor** tab to see the log messages that indicate which applications have been blocked. By default, policies are configured to create a log message only when traffic is not allowed by the policy, so only messages about applications that are blocked appear in Traffic Monitor.

To see log messages for all applications that are detected, even if that traffic is not blocked, you can configure the policy to generate a log message for all allowed packets. In the example configuration file, the **Any-outbound** policy is configured to send a log message for all allowed packets.

To see this configuration setting:

- Double-click the **Any-outbound** policy.
The Edit Policy Properties dialog box appears for the Any-outbound policy.
- Select the **Properties** tab.
- Click **Logging**.
The Logging and Notification dialog box appears.



WatchGuard System Manager also includes other reporting and monitoring tools that you can use to review Application Control log messages and create reports. For more information about logging and reporting, see the *Fireware XTM WatchGuard System Manager Help* at <http://www.watchguard.com/help/documentation/>.

Conclusion

In this configuration example, we explored how to add an XTM device to an existing network to block selected applications with Application Control. The addition of the XTM device to this network required no change to the existing firewall configuration, and no change to the configuration of any other devices on this network. The XTM device simply inspects the traffic and blocks the applications configured in the Application Control action.

After the XTM device is added to the network, it is easy to enable other security services that can increase the security of your network and your control over the content on the network. For example, you could enable **WebBlocker**, which allows you to block web content based on content categories, or **Intrusion Prevention Service**, which provides real-time protection from threats such as spyware, cross-site scripting, and buffer overflows.

For more information about the available WatchGuard XTM security services, see <http://www.watchguard.com/products/xtm-software/overview.asp>.

This configuration example blocks access to all Facebook applications, but you can also choose to selectively block some Facebook applications and allow others. For example, you can allow Facebook applications as needed by your Marketing department, but at the same time block access to the Facebook games.

For more information about how to get started with Application Control, see *Getting Started with Application Control* at [http://www.watchguard.com/help/docs/wsm/11-XTM/en-US/Application_Control_Getting_Started_\(en-US\)_V11_4_1.pdf](http://www.watchguard.com/help/docs/wsm/11-XTM/en-US/Application_Control_Getting_Started_(en-US)_V11_4_1.pdf)

About this Configuration Example

This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.

For complete product documentation, see the *Fireware XTM WatchGuard System Manager Help* or *Fireware XTM Web UI Help* on the WatchGuard web site at: <http://www.watchguard.com/help/documentation/>.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright © 1998-2011 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at: <http://www.watchguard.com/help/documentation/>.

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

