



OKENA  
71 Second Ave., 3<sup>rd</sup> Floor  
Waltham, MA 02451

Phone 781 209 3200  
Fax 781 209 3199

# StormWatch<sup>™</sup>

## Restrictive DNS Server Module

---

The policies shipped with StormWatch address both application-specific and environment-specific needs for servers and clients. In most cases, you'll want to use an application-specific policy in combination with an environment-specific policy to lock down a system with rules that are as restrictive or permissive as your network requires.

This document describes the module shipped with the StormWatch Management Console for protecting DNS servers. Use this document to understand what this policy currently does and then decide if it suits your network's needs.

NOTE: This policy does not protect the server system itself and it should be used in combination with other policies, such as the Server Module.

Policy Name	Policy Description
Restrictive DNS Server Module	V2.1 restrictive policy module for DNS servers

## Policy Description

This section contains descriptions of the rules included in the module recommended for deployment on DNS servers.

<b>Restrictive DNS Server Module</b>	V2.1 restrictive policy module for DNS servers
--------------------------------------	--

This policy allows administrators to secure DNS servers.

**1. File Access Control– Allow, MS Management applications, read/write DNS data files**

This rule allows local management of the DNS server using Microsoft Management Console.

**2. File Access Control– Allow, DNS server applications, read/write DNS data files**

This rule allows the DNS server read and write to its own data files. This access is locked down by the deny rule in this policy. This rule opens a targeted channel for DNS to access the resources it requires.

**3. Network Access Control – Allow, DNS server, server for DNS service**

This rule allows the DNS server application to act as a server for the DNS service. (Note that if you use this policy in combination with the Network Lockdown Module, this access is blocked. This rule, in effect, opens one specific channel and allows others to remain locked down.)

**4. Network Access Control – Allow, All applications, client for DNS service**

This rule allows all applications to act as a client for the DNS service. (Note that if you use this policy in combination with the Network Lockdown Module, this access is blocked. This rule, in effect, opens one specific channel and allows others to remain locked down.)

**5. File Access Control – Deny, All applications, write DNS data files**

This rule stops all applications from modifying specified DNS server data files. The allow rules in this policy open targeted channels within this deny rule to let only the DNS service access the files it needs.