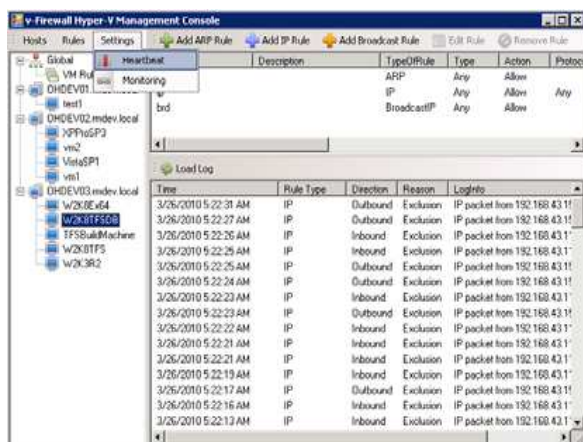


5nine Virtual Firewall for Microsoft Hyper-V

Version 2.1



Summary

5nine Virtual Firewall (v- Firewall) allows managing programmatically network security of Hyper-V Virtual Infrastructure on per-VM basis, defining network traffic rules for Hyper-V Virtual Machines, and hardening your Virtual environment from Security perspective. Virtual Firewall allows reviewing network traffic logs for each of the monitored Virtual Machines (VMs), and build related reports. 5nine Virtual Firewall also provides an ability of bandwidth throttling on per- VM basis.

Controls Network Traffic

Using simple **PowerShell API**/scripts or intuitive Management application an administrator can define/modify various firewall rules to allow or restrict various types of network traffic coming from the external network to Hyper-V virtual machines, or vice versa, **and between the virtual machines**. It allows protecting the Virtual

- Harden your Hyper- V VMs/VPS
- Control traffic for your VMs/VPS
- Set Network traffic rules with PowerShell API or GUI
- Block unwanted events

Machines and the Host System from both 'outside' and 'inside' vulnerabilities.

Deployment options

5nine Virtual Firewall can be used with Microsoft System Center Virtual Machine Manager templates when virtual machine is provisioned on Hyper-V / Server 2008 host, or to be deployed on the physical machine(s) prior to P2V Migration.

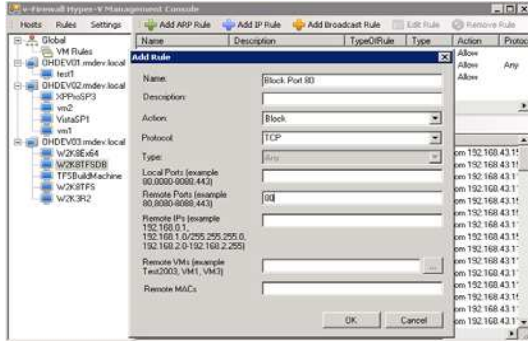
"Unlike traditional hardware firewalls, 5nine v-Firewall for Hyper-V allows us to programmatically manage network security on a per VM basis. Ultimately, this will decrease management costs and improve the security and compliance of our MaxV Cloud Servers" - Ryan Jones, Maximum ASP, Microsoft's Hosting Partner of the Year.

Compliance Audits

Enables successful compliance audits by providing the ability to monitor, report on, and filter virtual network traffic effectively

Firewall Rules

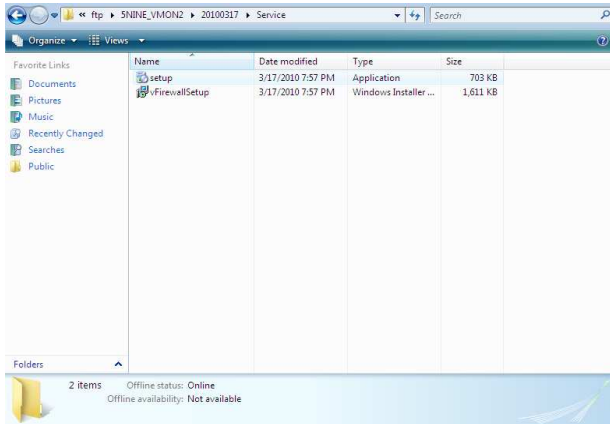
Using intuitive GUI an administrator can define Firewall rules to allow or restrict various types of network traffic coming from the external network to Hyper-V Virtual Machines, or vice versa. There are certain default rules set in the system, such as allowing all of the outbound traffic or blocking all of the incoming traffic to VMs from outside, except broadcasts.



Installation

5nine v-Firewall Management application can be installed either on a standalone server, or a Virtual machine with the following WinOS: Vista, Windows7, and Server 2008/R2w or later; x86 or x 64. Installation process is very simple:

- 1.) Management application should be installed running setup.exe from v-Firewall 2.0/Service directory in the installation package:



NET v3.5 SP1 and MS PowerShell are required on the Management server (or VM).

- 2.) Agents should be installed on VMs (VPS-es) using autorun.exe from /Agent directory in the installation package. Installation of the agents can be automated using simple script and Group Policies.

We recommend High Availability Management server (or VM) to have enough capacity, e.g., at least 4 processors, and to have at least **Max{4GBs, 5MBs x Amount of Virtual Machines}+** of RAM in Management server / VMs. Or, better --> **Max{4GBs, 10MBs x Amount of Virtual Machines}+**. So , for an environment of 1000+ VMs we recommend at least 8 - 16 GBs of RAM for an instance of the Management application.

Smaller environments can use 4 - 8 GBs of RAM for Management Servers/VMs.

After v-Firewall is installed - desired hosts and VMs need to be added for Monitoring, Security Heartbeat and Anti-Virus in 'Settings' menu of the Console.

Please refer to v-Firewall ' How to Use' Video for details.

Subsequently rules can be set either via Management application or using PowerShell API documented in Getting Started Guide.

```
Add-IP-Rule
Add-IP-Rule -VMId <Guid> -Name <String> [-Description <String>] [-
Type <String>] -Action <RuleAction> -Protocol <String> [-LocalPort
s <String>] [-RemotePorts <String>] [-IPAddresses <String>] [-VMs
<String>] [-MACAddresses <String>] [-Priority <Int32>] [-ApplyNow]
[-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningActi
on <ActionPreference>] [-ErrorVariable <String>] [-WarningVariab
le <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

```
Set-Heartbeat
Set-Heartbeat -VMId <Guid> -Enable 1|0 [-Verbose] [-Debug] [-ErrorActi
on <ActionPreference>] [-WarningAction <ActionPreference>] [-Error
Variable <String>] [-WarningVariable <String>] [-OutVariable <Stri
ng>] [-OutBuffer <Int32>]
```

```
Set-VMMonitoring
Set-VMMonitoring -VMId <Guid> -Enable 1|0 [-Verbose] [-Debug] [-ErrorA
ction <ActionPreference>] [-WarningAction <ActionPreference>] [-Er
rorVariable <String>] [-WarningVariable <String>] [-OutVariable <S
tring>] [-OutBuffer <Int32>]
```

Scalability and Performance

5nine v-Firewall has been tested both on Small, SMB, and Enterprise/Hosting - scale Hyper-V environments with >> than 1000s of VMs.

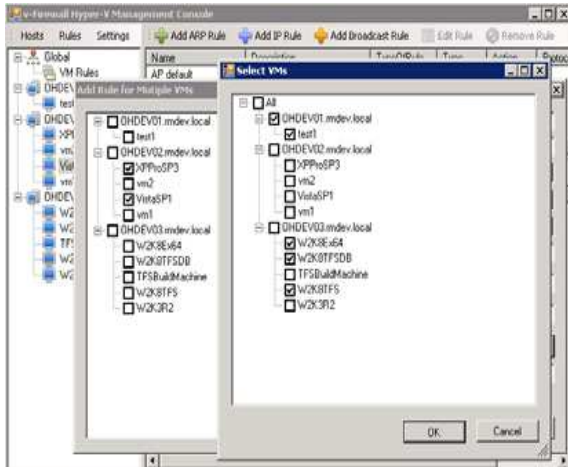
Performance measurements are as follows: with the Management application installed on 4 processor

server/VM, with 16GBs or more RAM, and with > 1000 monitored VMs - creation of Global rule (that applies to all VMs) took less than 1 min; individual VM rules update takes 2 - 3 secs. During checking the agents or updating the rule - memory used per VM has not ever exceeded 10 MBs.

This 5nine v-Firewall performs really well on both SMB and large scale Virtual environments, when properly configured, and when recommendations for the Management application are met.

Common Scenarios

5nine v-Firewall provides an ability to create rules in Management application or via PowerShell scripts to provide for Common scenarios such as Port80 traffic, RDP, FTP, etc. By default all traffic from/to and between Virtual machines is blocked, unless specific 'Allow' rules are created via the Console or API/Scripts.



Please refer to 5nine v-Firewall Getting Started Guide for examples of the common traffic filtering scenarios.

Security Heartbeat Service

Special service continuously checks if the network traffic rules are enforced, and can stop or pause the virtual machine if its network filter is not communicated to ensure that VM is not compromised.

System Requirements

- Microsoft Hyper-V Virtual environment;
- Vista SP1 (Business, Enterprise or Ultimate editions), Win 2003 R2 SP2, Win 2008 or later High Availability Virtual Machine or physical machine for v-Firewall Management interfaces;
- Microsoft PowerShell on Management Machine;
- .NET 3.5 SP1 or higher on Management Machine.

Ordering information and Support

Please visit www.5nine.com or contact sales@5nine.com for pricing information or a free trial.

For technical support, please visit <http://www.5nine.com/support.aspx> or e-mail techsupport@5nine.com and our support Representative will contact you promptly.

5nine Software

910 Foulk Road, Suite 201
Wilmington, Delaware 19803 USA

Sales@5nine.com
