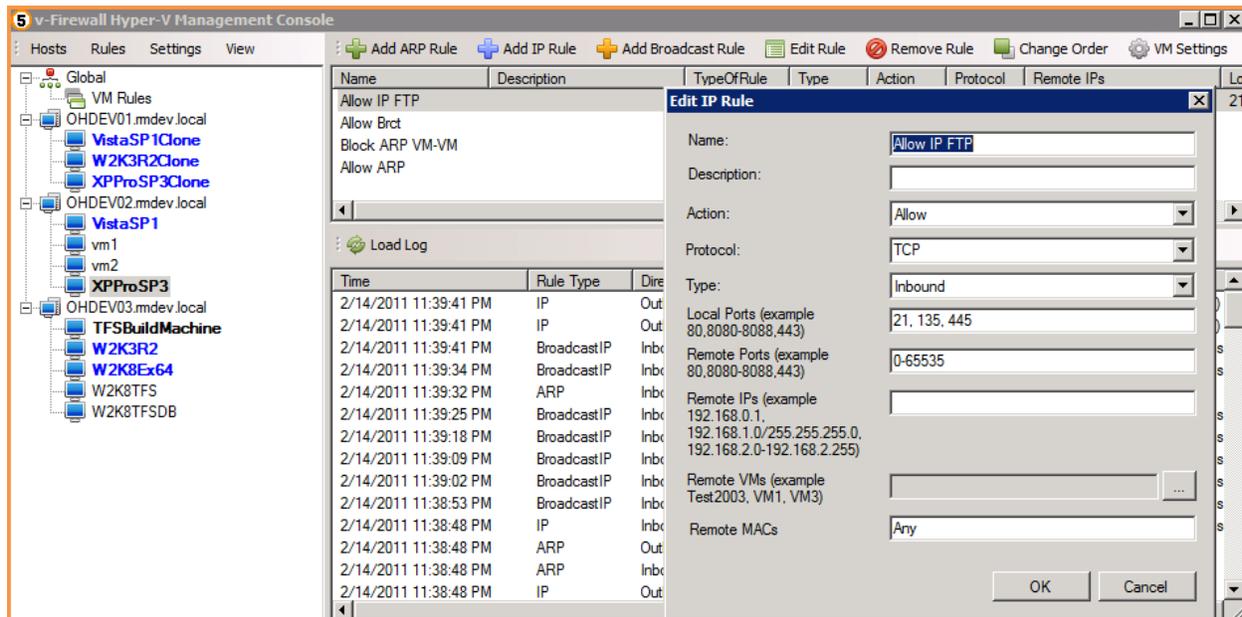


5nine Virtual Firewall 2.1 for Microsoft Hyper-V

KEY POINTS

- **Secure** your Hyper-V Virtual Machines & Virtual Servers
- **Control** Network Traffic In and Out of Your Virtual Machines & Virtual Servers
- **Restrict** Virtual Network Traffic Using Stateful Packet Filtering
- **Restrict** Network Traffic with Rules, Created with PowerShell or a Windows GUI
- **Block & Log** Malicious Network Traffic to **Prevent Downtime** for your Users & Applications



SUMMARY

5NINE Virtual Firewall (v-Firewall) allows you to programmatically manage the network security of your Hyper-V virtual infrastructure on per-VM basis, defining network traffic rules for Hyper-V virtual machines, and hardening the security of your virtual infrastructure.

Virtual Firewall allows you to log and analyze network traffic logs for each of the monitored Virtual Machines (VMs), allowing you to prove the security of the virtual infrastructure. Finally, 5NINE Virtual Firewall provides you the power to control the bandwidth utilization of each virtual machine in your infrastructure, preventing overutilization and denial of service to critical applications.

WHY YOU NEED VIRTUAL FIREWALL

The built-in Windows Firewall can protect your Hyper-V server but it won't do anything for your virtual machines. Virtual Firewall is the ONLY firewall available for Hyper-V. The packet filtering rules of v-Firewall allow you to permit only the traffic needed in and out of your virtual machines. With more and more critical applications and hosted virtual machines running in Hyper-V, it's more critical than ever

5nine Virtual Firewall 2.1 for Microsoft Hyper-V

before that you protect your Hyper-V infrastructure both from malicious attack as well as from misbehaving end-users.

CUSTOMER TESTIMONIAL

"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 MaxVCloud Servers"

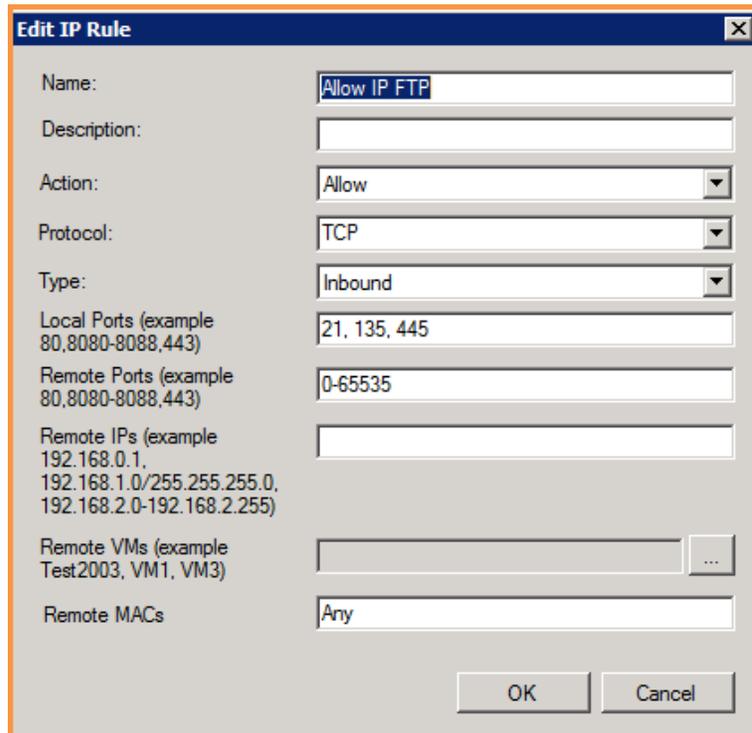
- Ryan Jones, Maximum ASP, Microsoft's Hosting Partner of the Year

CONTROL NETWORK TRAFFIC

With a few clicks of your mouse or a simple PowerCLI command, you can use v-Firewall to create & modify firewall rules. These rules allow you to restrict various types of network traffic coming from the external network (inbound) to the Hyper-V virtual machines, or from the virtual machines to the external network (outbound), or between VMs on the private virtual network. Thus, v-Firewall allows you to protect your virtual infrastructure from both 'outside' and 'inside' network attacks.

EASILY CREATE FIREWALL RULES

Firewall rules can easily be created across one or multiple virtual machines in the Hyper-V virtual infrastructure with a simple, intuitive interface. Creating a firewall rule is as easy as filling in the blanks of the windows shown in the graphic, below. Like traditional firewall rules, v-Firewall rules are based on source and destination IP addresses, protocols, and port numbers. However, unlike traditional firewalls, with v-Firewall you can create rules based on specific Hyper-V virtual machine names and apply those rules to one or more Hyper-V virtual machines. As soon as v-Firewall is installed the virtual machines are protected by default because there is an implicit "deny all" rule for all inbound and outbound traffic. From there, the administrator could quickly use default rules to, for example, allow all outbound traffic to the external network and accept inbound traffic that was a response to the outbound request (using the stateful firewall feature of v-Firewall).



Field	Value
Name:	Allow IP FTP
Description:	
Action:	Allow
Protocol:	TCP
Type:	Inbound
Local Ports (example 80,8080-8088,443)	21, 135, 445
Remote Ports (example 80,8080-8088,443)	0-65535
Remote IPs (example 192.168.0.1, 192.168.1.0/255.255.255.0, 192.168.2.0-192.168.2.255)	
Remote VMs (example Test2003, VM1, VM3)	
Remote MACs	Any



5nine Virtual Firewall 2.1 for Microsoft Hyper-V

AUDITING FOR COMPLIANCE

v-Firewall gives you the ability to prove compliance of your virtual infrastructure as it is the only tool of its kind that can monitor, report on, and filter Hyper-V virtual network traffic. Even if you don't have legal or auditory compliance requirements, you still need v-Firewall to provide logging and reporting of the traffic on the virtual network.

FLEXIBLE DEPLOYMENT OPTIONS

5NINE Virtual Firewall can be easily deployed either through the v-Firewall Management Application or programmatically through PowerShell API. Or, if you are using Microsoft System Center Virtual Machine Manager (SCVMM) templates you could deploy v-Firewall when a virtual machine is provisioned on a Hyper-V host.

SCALABILITY AND PERFORMANCE

5NINE v-Firewall has been thoroughly tested in Hyper-V environments at a variety of companies ranging in size from a small SMB all the way up to a large enterprise. Additionally, v-Firewall has been tested in the virtual infrastructure of hosting companies that have thousands of virtual machines. Based on this experience, we have determined that v-Firewall scales easily and performs well at even the largest company.

For example, at a large enterprise who had more than 1000 monitored virtual machines, creation of a global rule (which applied to all virtual machines) took less than 1 minute. At the same company, creation of a individual virtual machine rule took only 2-3 seconds. Even while updating the firewall rule, the v-Firewall agent on each VM didn't use more than 10MB of RAM. Note that the customer was using the v-Firewall management application installed on a 4 processor server with 16GB of RAM.

COMMON SCENARIOS

5NINE v-Firewall is commonly used to lockdown Hyper-V virtual machines from every direction and log traffic that was permitted or denied. More specifically, Hyper-V admins typically create rules using, either in the v-Firewall management application or via PowerShell, that are used to allow network traffic like HTTP/HTTPS (80/443), RDP(3389), or FTP (20/21), and others. Additionally, v-Firewall is commonly used to perform bandwidth throttling on individual virtual machines or groups of VMs.

As soon as v-Firewall is deployed virtual machines are protected by default because all traffic from & to each virtual machines (as well as between virtual machines) is denied unless specific 'Allow' (permit) rules are created.

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

SECURITY HEARTBEAT SERVICE

A powerful feature of v-Firewall is the heartbeat service which continuously checks to see if the network traffic rules are being enforced. This service can stop or pause the virtual machine if that VM's network filter is not communicating. By doing this, v-Firewall is able to ensure that the VM is not compromised.

5nine Virtual Firewall 2.1 for Microsoft Hyper-V

SYSTEM REQUIREMENTS

- Microsoft Hyper-V virtual infrastructure
- Vista SP1 (Business, Enterprise or Ultimate editions), Win 2003 R2 SP2, Win 2008 or later with high availability features
- Virtual machine or physical machine for v-Firewall management interfaces
- Microsoft PowerShell installed on the management VM
- .NET 3.5 SP1 or higher on the management VM

INSTALLATION

Installation of the 5NINE v-Firewall Management application is quick and easy

Hyper-V v-Firewall can be installed either on a standalone server or a virtual machine with using one of the following as the base OS:

- Windows Vista
- Windows7
- Server 2008/R2 or later with x86 or x64

Add-IP-Rule

```
Add-IP-Rule -VMId <Guid> -Name <String> [-Description <String>] [-Type <String>] -Action <RuleAction> -Protocol <String> [-LocalPorts <String>] [-RemotePorts <String>] [-IPAddresses <String>] [-VMs <String>] [-MACAddresses <String>] [-Priority <Int32>] [-ApplyNow] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Set-Heartbeat

```
Set-Heartbeat -VMId <Guid> -Enable 1|0 [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Set-VMMonitoring

```
Set-VMMonitoring -VMId <Guid> -Enable 1|0 [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Here's the simple Installation instructions for v-Firewall:

- 1.) On the virtual or physical server you designate as the management application server, simply run **setup.exe** from the ZIP file you downloaded. Make sure that you have NET v3.5 SP1 and MS PowerShell which required on the Management server (or VM)
- 2.) Install **agents** on VMs the using autorun.exe from /Agent directory in the installation package. Installation of the agents can be automated using simple script and Group Policies.

In order to size the VM properly, we recommend 1000+ VMs we recommend at least 8 - 16 GBs of RAM for an instance of the management application whereas smaller environments can use 4 - 8 GBs of RAM for Management Servers/VMs.

After v-Firewall is installed, you'll find - desired hosts and VMs need to be added for Monitoring, Security Heartbeat and Anti-Virus in **Setting** menu of the Console. Please refer to v-Firewall **How to Use** Video for details. Once installed, subsequently rules can be set either via Management application or using PowerShell API documented in **Getting Started Guide**.

©2011 5nine Software, Inc. The information contained herein is subject to change without notice. 5nine shall not be liable for technical or editorial errors or omissions contained herein.



5nine Virtual Firewall 2.1 for Microsoft Hyper-V

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:

- Our website at <http://www.5NINE.com/support.aspx>
- Or contact us via e-mail at techsupport@5NINE.com

Our support representatives will contact you promptly.