5NINE SOFTWARE

Manage and Protect
the Microsoft Cloud Platform

WHITE PAPER

5nine Cloud Security Hardens Virtual Machines (VMs) Across Windows Server 2016 and Microsoft Azure

Konstantin Malkov
Chief Technology Officer and Director

Microsoft Partner
Gold Datacenter

INTRODUCTION

Information security incidents at large companies and government agencies have recently become regular occurrences. Increased security requirements and federal mandates have pressured organizations to build their own virtual infrastructures, but often they use outdated agent-based endpoint security and private VLANs to secure their virtual environment. These methods create vulnerabilities linked to the ability to block or delete the agent in the VM.

Agent-based endpoint security consumes scarce hardware resources and complicates the administration of virtual data centers. To be successful, businesses must be able to rapidly create and securely maintain new services and the virtual machines that comprise them, and support multiple clusters or datacenters, while migrating and balancing VMs between them. Cloud architecture is the best solution.

Changing Business Environment

Virtualization and Cloud solutions have been growing steadily for many years. A recent Gartner Analysis showed, that at the end of 2016, more than 75% of corporate workloads were virtualized. Simultaneously, hypervisor capabilities have expanded and transformed into private, public and hybrid clouds. As a result, infrastructures have become more flexible and dynamic, in sync with today’s modern business requirements, and security has become increasingly important.

HOW DOES THE MICROSOFT 'INTELLIGENT CLOUD' IMPROVE INFRASTRUCTURE SECURITY?

1. Protection via Shielded VMs

To protect against the "Snowden effect", Windows Server 2016 features 'Shielded VMs', which make it possible to encrypt a VM's hard disk on guest operating systems, protecting it from being copied and viewed by the host administrator or other users. Businesses are also encouraged to use BitLocker in guest VMs.

2. Minimizes roles with Nano Server

Data center security is significantly improved by using Nano Server, a new OS that lacks a GUI and significantly reduces the attack surface by minimizing the set of roles. As a result, there are 3 times fewer ports and 10 times fewer critical updates. Another innovation is protection for components responsible for the integrity of the OS kernel, passwords, and other important system data when using a separate container in Hyper-V Virtual Secure Mode (VSM). All of this significantly increases the security of the new OS and users' infrastructures.

3. Enhanced Security using Hyper-V Switch Extensions

Datacenters often lack several important security and compliance functions since they are not standard features in server operating systems, or are very complex to implement. Thus Microsoft has made it significantly easier for ISVs to implement these functions by giving several partners access to the Hyper-V switch. The extensible Hyper-V virtual switch makes it possible to isolate VM users, manage all traffic within the virtual environment, and protect VMs against malicious attacks. Thanks to built-in support for NDIS Filter Drivers, the extensible Hyper-V virtual switch allows authorized ISVs to create virtual switch extensions (such as filtering or forwarding extensions) that increase VM and network security or perform various monitoring and reporting functions(via capturing extensions).

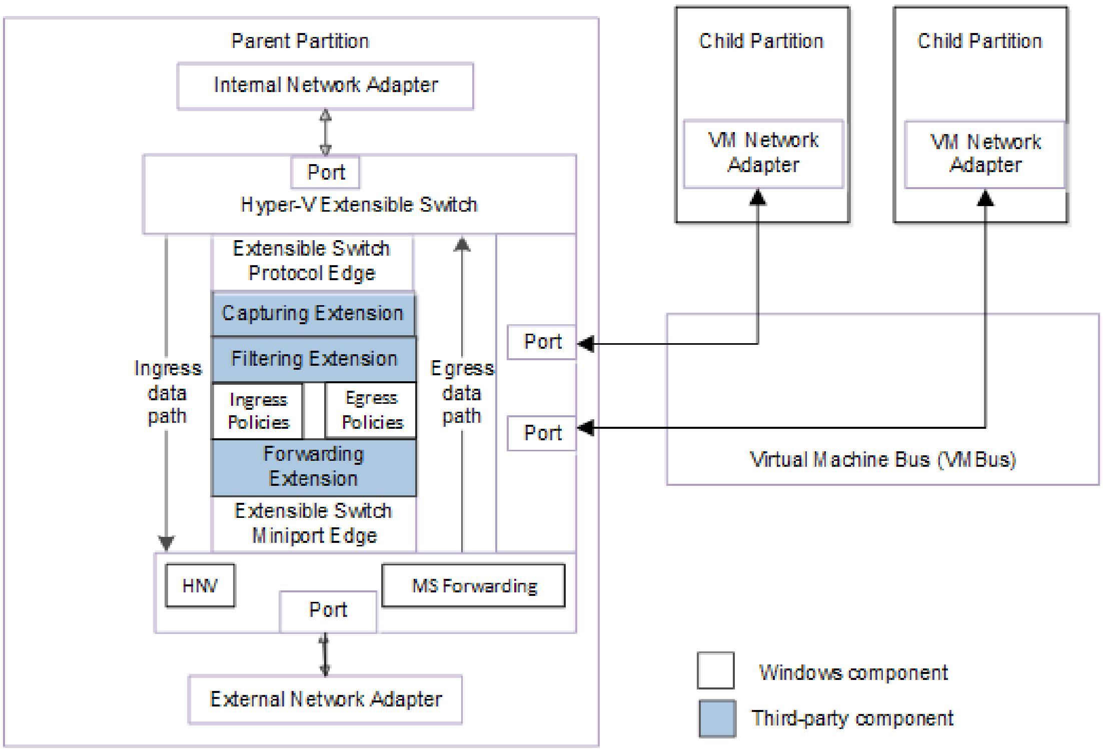


Figure 1: Schematic overview of Hyper-V Extensible Switch

Source: https://msdn.microsoft.com/en-us/windows/hardware/drivers/network/overview-of-the-hyper-v-extensible-switch

HOW DOES 5NINE SOFTWARE LEVERAGE THE HYPER-V SWITCH TO HARDEN VMS ACROSS MICROSOFT'S HYBRID CLOUD?

In many cases, Windows Server 2016 or Microsoft Azure is selected as the virtualization platform of choice: its cost-efficiency and powerful feature set differentiate it from competing platforms. 5nine Software has participated in many of these projects and is recognized as a leader in hardening VMs across Microsoft's Hybrid Cloud.

Since 2010, 5nine Software has been collaborating with Microsoft to develop Hyper-V security and management tools. The latest version of 5nine Cloud Security, which was unveiled simultaneously with Windows Server 2016 at the annual Ignite conference, was greeted with enthusiasm by networking and security professionals.

5nine Cloud Security is integrated with the virtual switch and is the only patent-pending, completely agentless security solution for Windows Server Hyper-V. It monitors network traffic between virtual machines, isolates individual VMs and groups, detects malicious attacks at the application level, and performs rapid anti-virus scans and threat blocking, thus increasing the security of the virtual environment.

The solution's agentless architecture, which eliminates the need to install software on the guest operating system and makes it possible to analyze and control traffic at the virtual switch level, sets it apart from other information security tools.

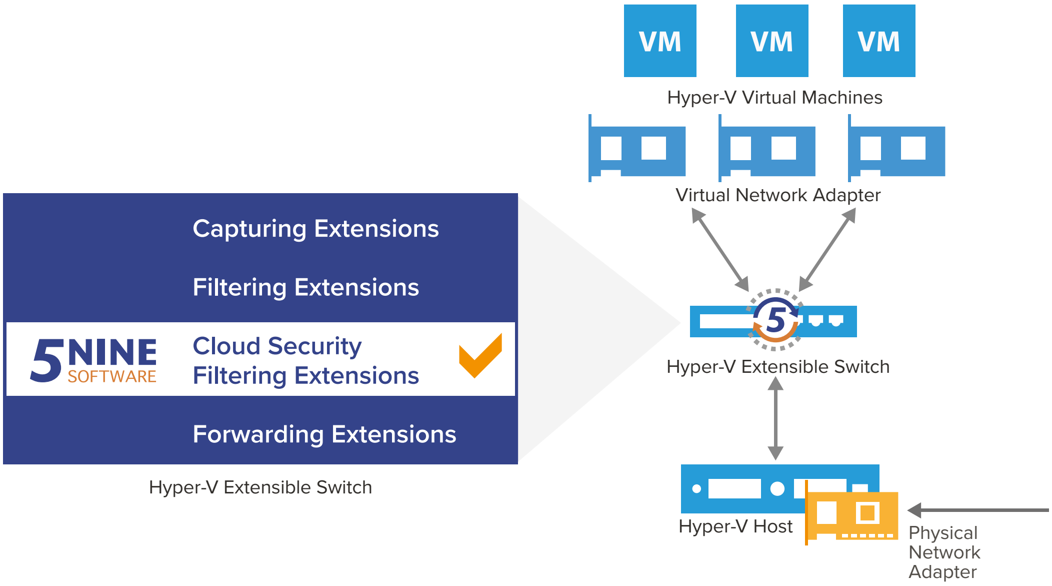


Figure 2: How 5nine Cloud Security leverages the Hyper-V extensible switch

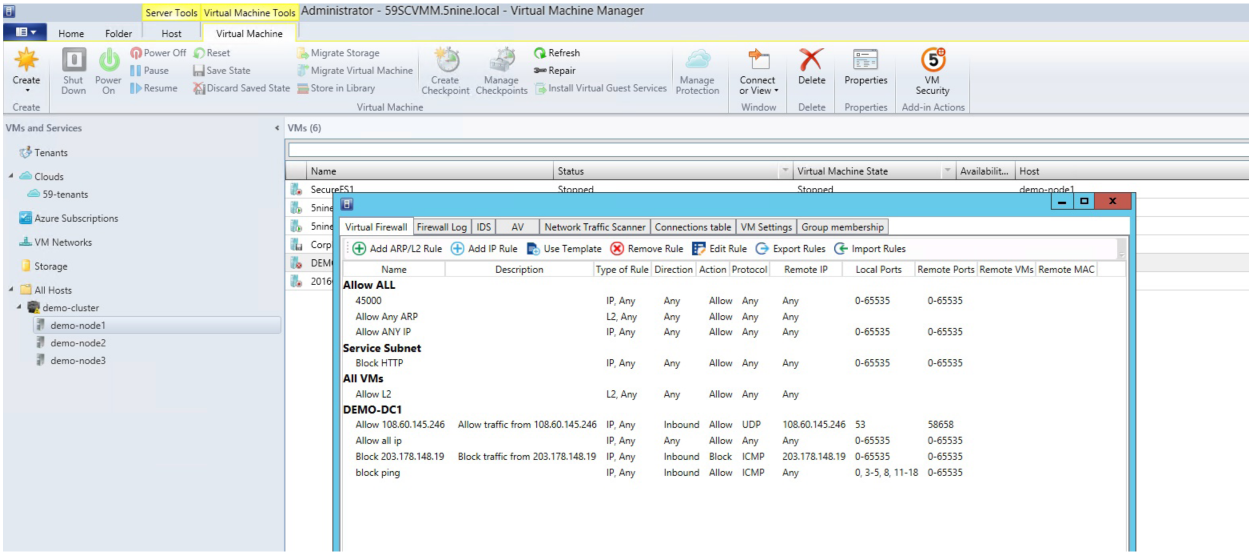
Features Easy, 3 Component Installation

5nine Cloud Security can be easily installed by a Windows Server administrator with skills equivalent to an MCSA. Competing solutions are significantly more complex and expensive, requiring more effort and proficiency to install.

- Management Service – This component is installed on the guest or parent partition that will be designated as the managing server for all Hyper-V infrastructures. You can install several managing servers to provide emergency recovery.
- Host Management Service – This component is installed on each server being protected.
- Management Console – This component is installed on each workstation or VM used to manage and monitor the application.

Allows Integration with System Center Virtual Machine Manager (SCVMM)

5nine Cloud Security can also be integrated with SCVMM. Users can install a free plugin which allows them to manage their data center infrastructure and virtualization security from a single SCVMM console. The combined solution makes it easier and less expensive to use Microsoft Cloud in 'on premise' data centers and allows monitoring and management of infrastructure security in a hosting company's cloud built on Cloud OS.Cloud OS.



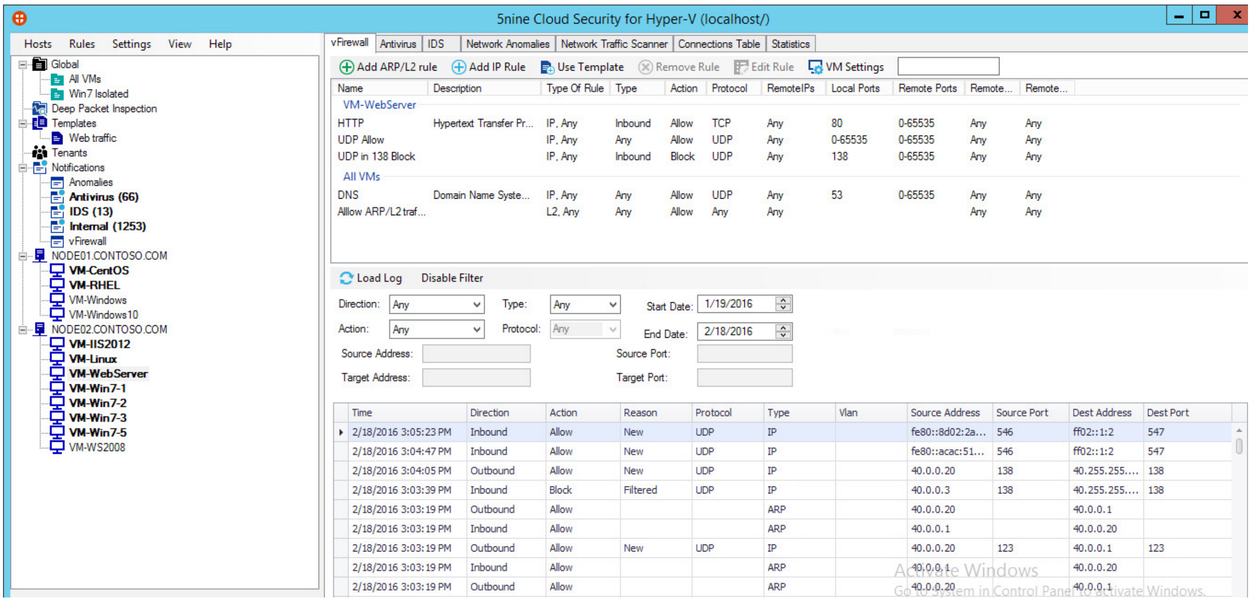
Name	Description	Type of Rule	Direction	Action	Protocol	Remote IP	Local Ports	Remote Ports	Remote VMs	Remote MAC
Allow ALL										
45000		IP, Any	Any	Allow	Any	Any	0-65535	0-65535		
Allow Any ARP		L2, Any	Any	Allow	Any	Any				
Allow ANY IP		IP, Any	Any	Allow	Any	Any	0-65535	0-65535		
Service Subnet										
Block HTTP		IP, Any	Any	Allow	Any	Any	0-65535	0-65535		
All VMs										
Allow L2		L2, Any	Any	Allow	Any	Any				
DEMO-DC1										
Allow 108.60.145.246	Allow traffic from 108.60.145.246	IP, Any	Inbound	Allow	UDP	108.60.145.246	53	58658		
Allow all ip		IP, Any	Any	Allow	Any	Any	0-65535	0-65535		
Block 203.178.148.19	Block traffic from 203.178.148.19	IP, Any	Inbound	Block	ICMP	203.178.148.19	0-65535	0-65535		
block ping		IP, Any	Inbound	Allow	ICMP	Any	0, 3-5, 8, 11-18	0-65535		

Figure 3: 5nine Cloud Security Home Screen

FEATURE-RICH FUNCTIONALITY DETAILED BELOW MAKE 5NINE CLOUD SECURITY THE TOOL OF CHOICE

Azure Pack Extension enables security as a service (SECaaS)

The Azure Pack extension enables management of Cloud Security functions from a self-maintained portal, allowing hosting companies roll out security as a service. The product implements a role-based model for managing security. Three roles are available: Information security administrator, IT administrator, and Auditor.



Name	Description	Type Of Rule	Type	Action	Protocol	RemoteIPs	Local Ports	Remote Ports	Remote...	Remote...
VM-WebServer										
HTTP	Hypertext Transfer Pr...	IP, Any	Inbound	Allow	TCP	Any	80	0-65535	Any	Any
UDP Allow		IP, Any	Any	Allow	UDP	Any	0-65535	0-65535	Any	Any
UDP in 138 Block		IP, Any	Inbound	Block	UDP	Any	138	0-65535	Any	Any
All VMs										
DNS	Domain Name Syste...	IP, Any	Any	Allow	UDP	Any	53	0-65535	Any	Any
Allow ARP/L2 traf...		L2, Any	Any	Allow	Any	Any			Any	Any

Direction: Any
Type: Any
Start Date: 1/19/2016
Action: Any
Protocol: Any
End Date: 2/18/2016
Source Address:
Source Port:
Target Address:
Target Port:

Time	Direction	Action	Reason	Protocol	Type	Vlan	Source Address	Source Port	Dest Address	Dest Port
2/18/2016 3:05:23 PM	Inbound	Allow	New	UDP	IP		fe80::8d02:2a...	546	ff02::1:2	547
2/18/2016 3:04:47 PM	Inbound	Allow	New	UDP	IP		fe80::acac:51...	546	ff02::1:2	547
2/18/2016 3:04:05 PM	Outbound	Allow	New	UDP	IP		40.0.0.20	138	40.255.255....	138
2/18/2016 3:03:39 PM	Inbound	Block	Filtered	UDP	IP		40.0.0.3	138	40.255.255....	138
2/18/2016 3:03:19 PM	Outbound	Allow			ARP		40.0.0.20		40.0.0.1	
2/18/2016 3:03:19 PM	Inbound	Allow			ARP		40.0.0.1		40.0.0.20	
2/18/2016 3:03:19 PM	Outbound	Allow	New	UDP	IP		40.0.0.20	123	40.0.0.1	123
2/18/2016 3:03:19 PM	Inbound	Allow			ARP		40.0.0.1		40.0.0.20	
2/18/2016 3:03:19 PM	Outbound	Allow			ARP		40.0.0.20		40.0.0.1	

Figure 4: 5nine Cloud Security Firewall Tab

Defined Individual and Group Firewall Options

Through the use of templates, an administrator can use his/her own console or the SCVMM to easily configure the security policy for the virtual firewall. Both Windows and Linux VMs are supported. Thanks to the multitenancy support, you can isolate both individual VMs and specific VM groups. Protection, including anti-virus protection, is available for the Hyper-V server's parent partition itself.

The firewall enables:

- MAC address filtering
- ARP support
- SPI (Stateful Packet Inspection) and DPI (Deep Packet Inspection)
- Analysis of network traffic anomalies using state of the art AI Supervised and Unsupervised machine learning along with behavioral pattern and anomaly analysis algorithms (UEBA)
- Management of inbound and outbound bandwidth for each virtual machine
- MAC broadcast filtering
- Logging of filtered security incidents (including anti-virus and IDS incidents) with the ability to export to SYSLOG and SIEM SPLUNK files
- Support for Software Defined Networking (SDN) technologies

Anti-virus Protection at the Hypervisor Level

The anti-virus service uses your choice of three engines and signature databases (Kaspersky Labs, Bitdefender, or Threat Track), but the scanning mechanism is fundamentally different than that used by the anti-virus vendors. Functionality is located at the hypervisor level so anti-virus scanning is possible without installing an agent on VMs. This makes them more secure, since the guest operating system's administrator cannot disable the anti-virus software. Incremental scanning technology makes scanning 70 times faster while also reducing the load on the host by up to 30%.

This technology combined with the ability to configure the number of VMs being scanned makes it possible to flexibly manage host resources and avoid an "anti-virus storm". There is also anti-virus scanning of network traffic and the option for active VM defense, which involves scanning not only hard disks, but also the guest partition's memory. Anti-virus and IDS signature databases can be centrally updated for the entire Hyper-V infrastructure through a local proxy server, making it possible to isolate hosts from public networks while simultaneously placing them in data centers to minimize parent partitions' vulnerabilities to external attacks.

The anti-virus service's interface provides the ability to configure and schedule the scanning mode and to exclude various file types and folders.

Intrusion Detection System (IDS) Stops Attacks From Within

The IDS analyzes all traffic within the Hyper-V virtual switch using Cisco Snort for Business to check packet anomalies, which may represent attacks. Unlike similar solutions from other vendors, 5nine Cloud Security can detect not only external attacks, but also attacks within the virtual environment from one VM to another. This type of attack has become more and more common in hosting companies' virtual data centers as well as at major companies, where one hijacked VM becomes the center for an attack from inside the lines of defense.

Network Analysis Identifies Anomalies

Attacks are not only detected using signatures, but also heuristics / behavior analytics. The Network Analysis module constructs a model of your normal network traffic during various time intervals. Then it continuously monitors your traffic profile and, if deviations or anomalies are detected, immediately reports the potential attack.

Advanced AI algorithms provide additional capabilities to alert system and security administrators regarding anomalies in various inbound and outbound traffic patterns and trends, including the time of the events, packet size, external and virtual network loads, etc.

Increased Support for Distributed Datacenters

Large companies will have the ability to migrate security policies to distributed data centers. If you have several data centers or branch offices that do not have direct communication links, you can still synchronize 5nine Cloud Security settings between them, thus supporting VM migration, fault tolerance, and business security in the event of an emergency.

Single Solution Compliance with Multiple Industry Standards

The presence of every protection system (virtual firewall, anti-virus, IDS, security incident logging, role-based access model) enables users in the Windows Server ecosystem to satisfy various security and compliance regulations. This includes PCI-DSS, HIPAA, and others.

Architectural Advantages Offer High Level of Security with Low Resource Load

Unlike competing solutions, 5nine Cloud Security is easy to use and install. It easily integrates with Microsoft's management tools, and configuration is fast and intuitive. The primary advantage is that the solution provides high security at the hypervisor level and low loads on host resources. Performance testing of 5nine Cloud Security with all services enabled shows that the additional load is 3-4%.

Tests of similar products from other venders show that virtual network bandwidth decreases by up to 50%. Additionally, testing of these products reveals that if the management service on a VM crashes, all important network settings are lost and the network becomes virtually unusable. When a VM with the 5nine management service is shut down, all settings are preserved and Cloud Security continues its uninterrupted protection of the virtual infrastructure.

Enterprise Ready and Scalable

For large companies with a Chief Information Security Officer (CSO), there is a fault-tolerant security mode with cluster-based management service and Recovery Action in order to restart after a crash. 5nine Cloud Security also supports disaster recovery of multiple physical sites, which is extremely important for the high availability of service providers and public sector data centers.

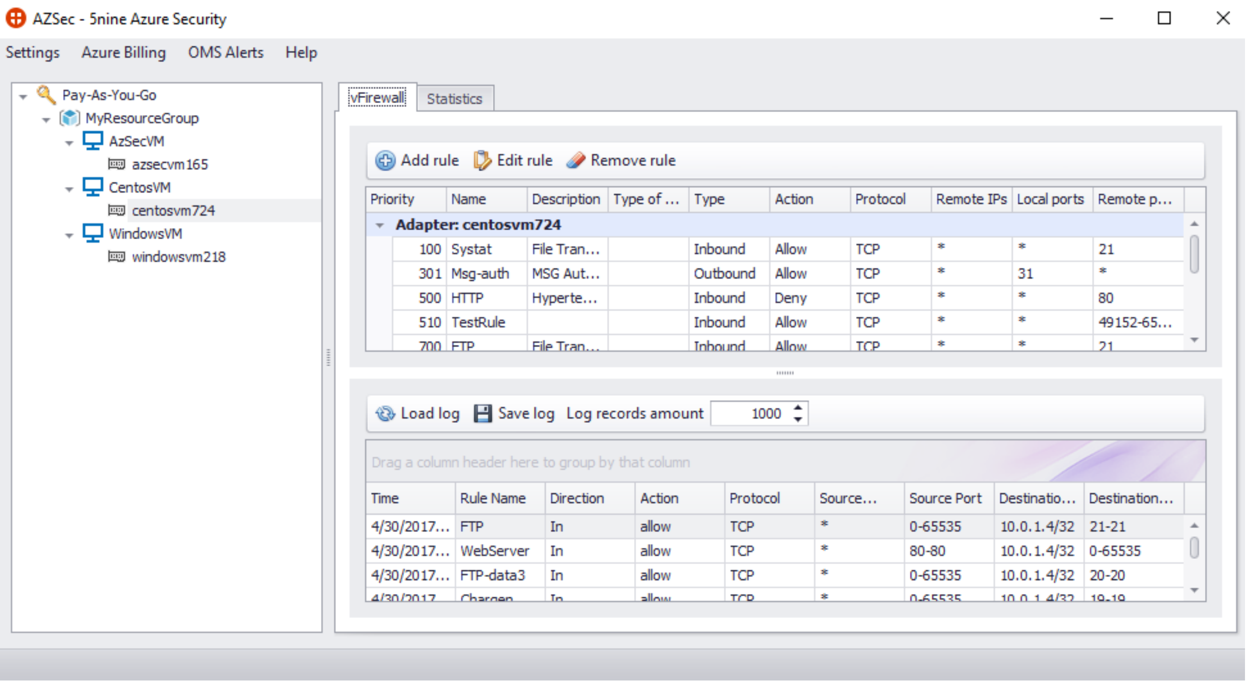
The recently added distributed management server function can optimize performance of 5nine Cloud Security managing services for large enterprises and make them more scalable. This technology allows several managing services to run simultaneously, and allows data center security rules and settings to be applied and edited. It also increases the fault tolerance and high availability of the 5nine services that provide comprehensive security to a virtual infrastructure with a complex topology, including geographically distributed infrastructure.

Depending upon the data center architecture, administrators can launch several management services in close proximity to the managed resources to more quickly distribute new security settings and change existing ones.

These settings are distributed to and synchronized between all managing services to facilitate flexible configuration. If a management service becomes unavailable, the group of hosts is switched to the closest working management service. An administrator may assign a specific managing service from a list of available services to each group of hosts. Once configured, the hosts exchange data with the assigned service in order to receive notifications, configurations, and logs analysis.

Recent 5nine Cloud Security Releases

The newly released 10.0 version of 5nine Cloud Security also provides the ability to create security/network traffic rules and seamlessly review, save and analyze logs for VMs running in Microsoft Azure using the same easy-to-use ‘on the fly’ interface found in the Private Cloud version. The result is the ability to manage hybrid clouds from one cohesive Security Suite.



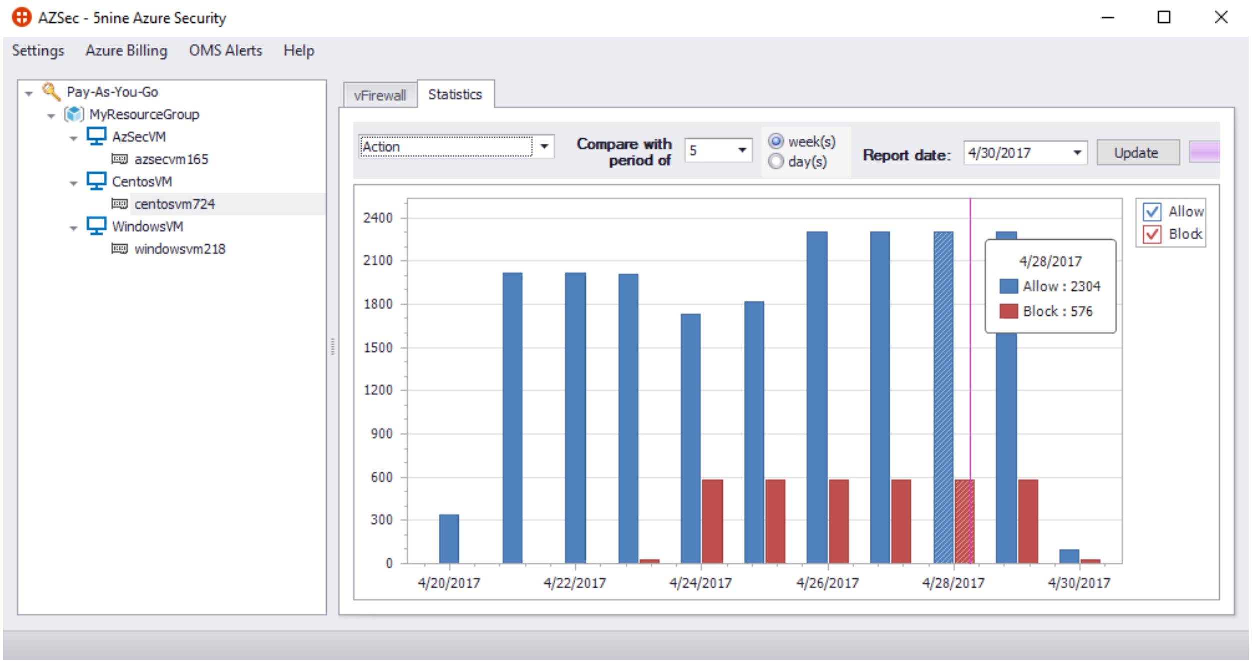
Adapter: centosvm724

Priority	Name	Description	Type of ...	Type	Action	Protocol	Remote IPs	Local ports	Remote p...
100	Systat	File Tran...		Inbound	Allow	TCP	*	*	21
301	Msg-auth	MSG Aut...		Outbound	Allow	TCP	*	31	*
500	HTTP	Hyperte...		Inbound	Deny	TCP	*	*	80
510	TestRule			Inbound	Allow	TCP	*	*	49152-65...
700	FTP	File Tran...		Inbound	Allow	TCP	*	*	21

Log records amount 1000

Time	Rule Name	Direction	Action	Protocol	Source...	Source Port	Destinatio...	Destination...
4/30/2017...	FTP	In	allow	TCP	*	0-65535	10.0.1.4/32	21-21
4/30/2017...	WebServer	In	allow	TCP	*	80-80	10.0.1.4/32	0-65535
4/30/2017...	FTP-data3	In	allow	TCP	*	0-65535	10.0.1.4/32	20-20
4/30/2017	Chargen	In	allow	TCP	*	0-65535	10.0.1.4/32	19-19

Figure 5: The new version of 5nine Cloud Security



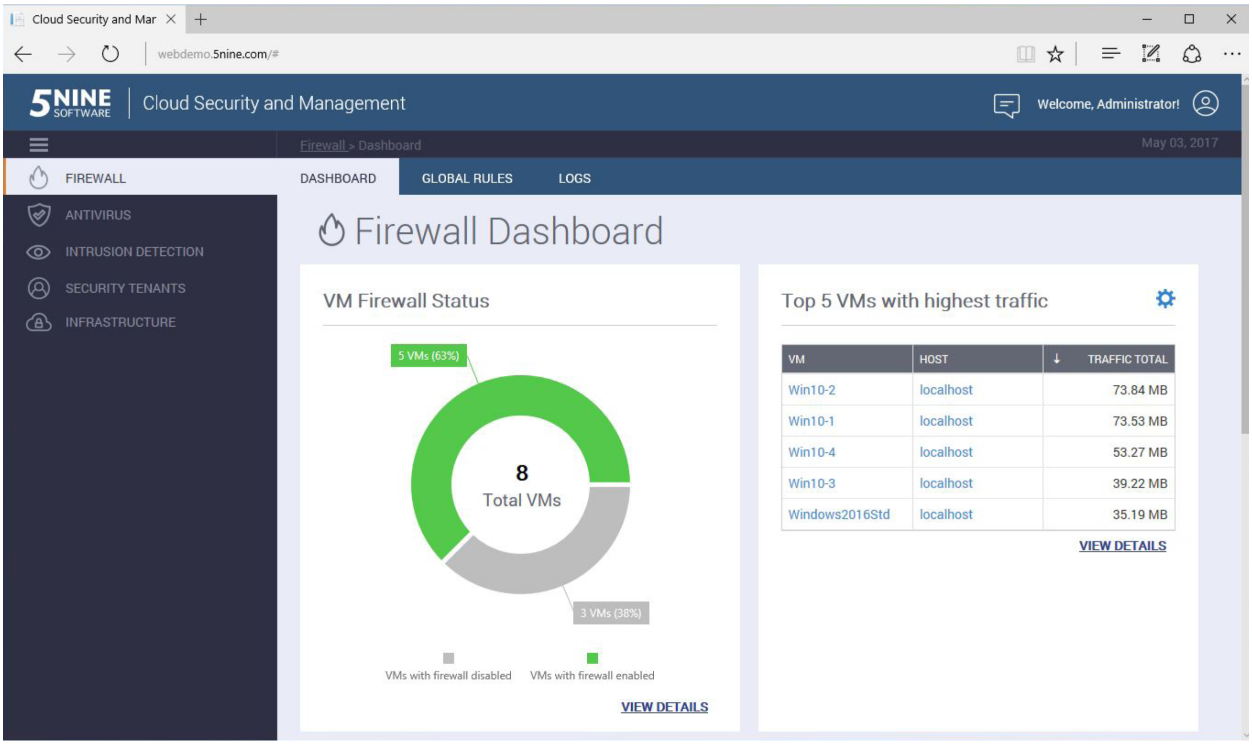
Action

Compare with period of 5 ● week(s) ○ day(s)

Report date: 4/30/2017

Figure 6: The new version of 5nine Cloud Security also integrates with Microsoft OMS.

Web – based Management and Security console will be released soon as well – it will allow to Manage Microsoft Cloud Security and infrastructure from the web browser(s), so no client side installation will be required:3



VM	HOST	↓ TRAFFIC TOTAL
Win10-2	localhost	73.84 MB
Win10-1	localhost	73.53 MB
Win10-4	localhost	53.27 MB
Win10-3	localhost	39.22 MB
Windows2016Std	localhost	35.19 MB

Figure 7: Web-based MAnagement and Security console

Conclusion

Using 5nine Cloud Security functions, customers reliably protect their Microsoft Cloud virtual infrastructure, regardless of size or complexity and comply with rigorous international information security and compliance standards. With no degradation of performance, they provide simple management of both documented and new (but undocumented) threats.

Next Steps

Cyber Defense Magazine named 5nine Cloud Security the best 2016 Data Center Security solution thanks to its unique capabilities. More than 100,000 customers around the world have already chosen 5nine Software solutions to secure and manage Microsoft Clouds.

Try 5nine Cloud Security today by installing our fully functional 30-day evaluation or by test-driving the solution in our virtual lab.

About the Author

Dr. Konstantin Malkov is the Chief Technology Officer at 5nine Software, where he manages design and development of 5nine Virtualization Security Management and Compliance products.

Previously Konstantin was a CTO for PWI, Inc. and privacyware.com, where he led the design of various security products - including ThreatSentry and PrivateFirewall.

Between 1998 and 2005 Dr. Malkov served as a CTO for Internet Transactions Solutions which was acquired by ORCC for $45 mln.

Konstantin has also managed numerous commercial software development projects in the field of messaging, workflow, business analytics and security for various world-class organizations including AT&T, Gillette Company, Lucent Technologies, IBM, EasyLink Services, Premiere Global Services, Webroot Software, and many others.

Dr. Malkov is a recognized, international scientist and is co-founder of the Department of Non-linear Dynamic Systems and Control at Moscow State University. He is a former professor of Applied Mathematics and Computer Science at Moscow State University and received his Ph.D in Applied Mathematics and Computer Science from that institution. Professor in Applied Mathematics (1990); Dr. Malkov has resided in the US since 1991.

About 5nine Software

5nine Software is the leading global Hyper-V virtualization security and management provider. We offer the first and only agentless security and management solutions for Microsoft Hyper-V. Our innovative, powerful and easy-to-use software is designed to reduce costs, increase productivity and mitigate security risks. Over 100,000 users trust 5nine Software to migrate, manage and secure their virtual infrastructure.

To learn more, visit http://www.5nine.com.

Sales:

Phone US: + 1 561-898-1100

Phone EU: + 44 (20) 7048-2021

Email: sales@5nine.com

Fax: + 1 732 203 1665

Technical Support:

Phone US/Canada Toll Free: + 1 877 275 5232

Email: techsupport@5nine.com

DOWNLOAD FREE TRIAL