

Interface to Network Security Functions

Nov 2014

Linda Dunbar (linda.dunbar@huawei.com)

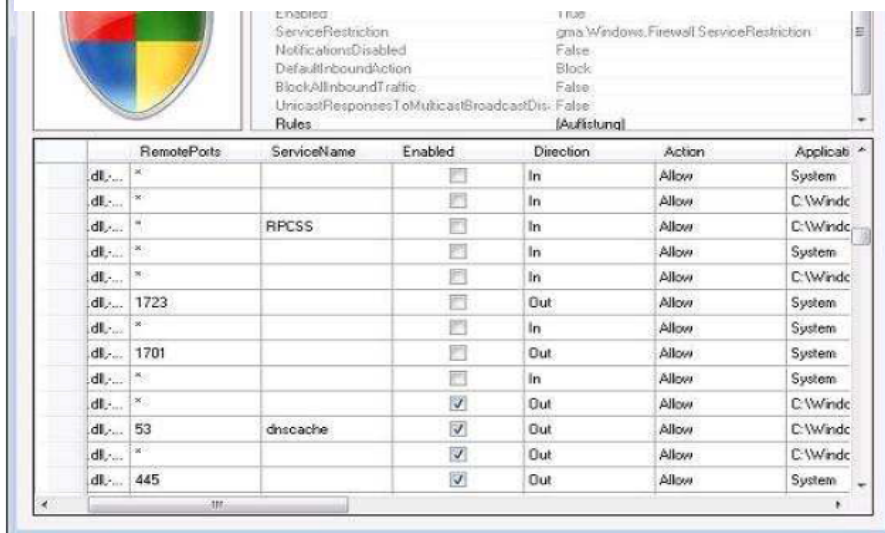
Myo Zarny (Myo.Zarny@gs.com)

Christian Jacquenet (Christian.jacquenet@orange.com)

Shaibal Chakrabarty (shaibalc@us-ignite.org)

Firewall box configuration: ports & links based

Firewall Rules Configuration								
Active	Type	Rule	Protocol	Source	Port(s)	Destination	Port(s)	Comments
No	Access	Permit	UDP	IP or Host Name 192.168.0.50	ALL	Any	53	Example - Permit DNS request to this IP
No	Access	Permit	TCP	IP or Host Name 192.168.0.50	ALL	Any	110	Example - Permit POP access to this IP
No	Access	Permit	TCP	IP or Host Name 192.168.0.50	ALL	Any	25	Example - Permit SMTP access to this IP
No	Access	Deny	ALL	IP or Host Name 192.168.0.50	ALL	Any	ALL	Example - Deny all access to this IP
No	Access	Deny	ALL	IP or Host Name 192.168.0.48/30	ALL	Any	ALL	Example - Deny access to this Sub-net
No	Access	Deny	TCP	Any	ALL	Any	21	Example - Deny access to FTP sites

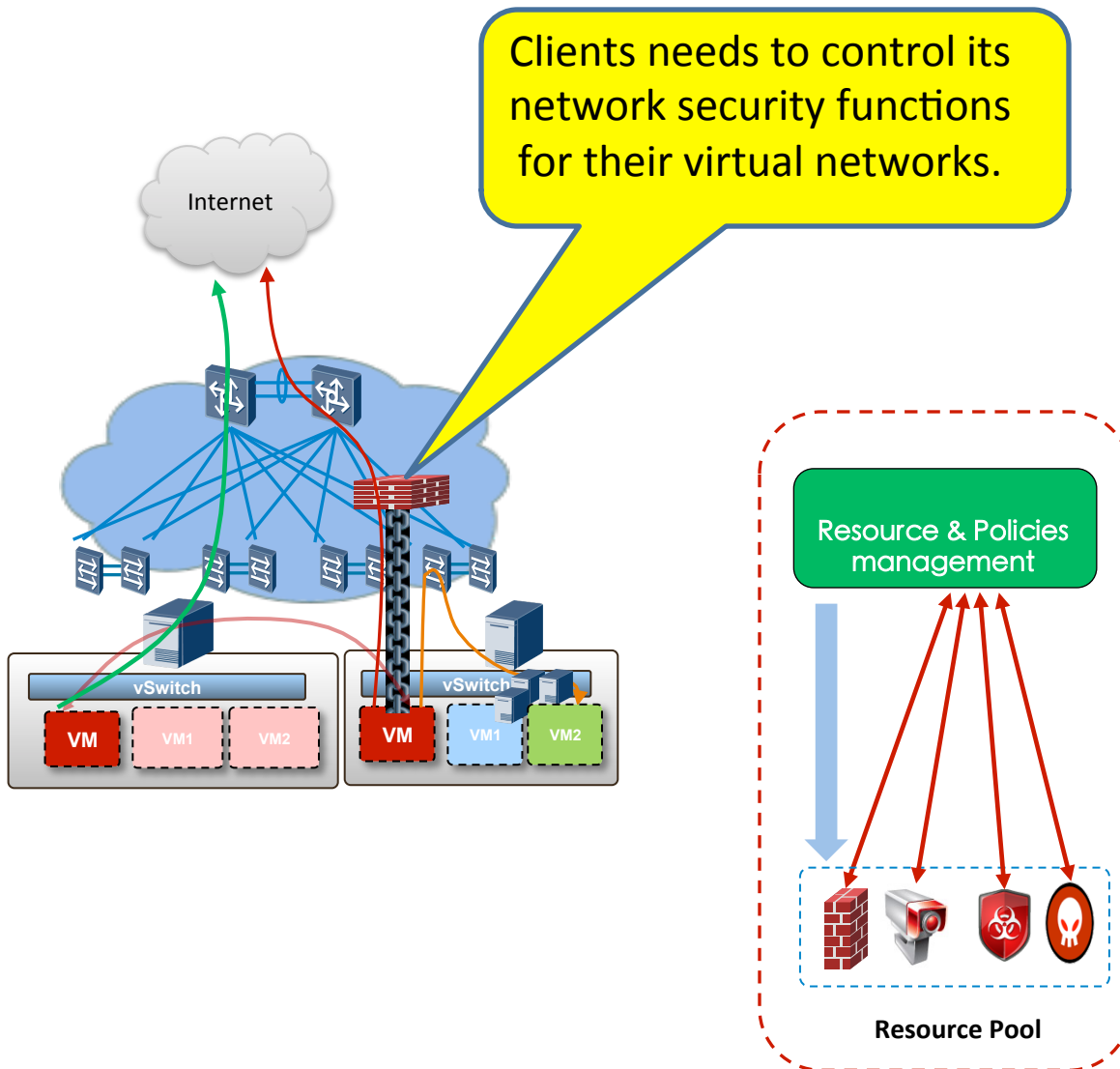


Enabled: 1 rule
 ServiceRestriction: gma\Windows\Firewall\ServiceRestriction
 NotificationsDisabled: False
 DefaultInboundAction: Block
 BlockAllInboundTraffic: False
 UnicastResponsesToMulticastBroadcastDis: False
 Rules: (Aufstunda)

RemotePorts	ServiceName	Enabled	Direction	Action	Applicati
dl...		<input type="checkbox"/>	In	Allow	System
dl...		<input type="checkbox"/>	In	Allow	C:\Windc
dl...	RPCSS	<input type="checkbox"/>	In	Allow	C:\Windc
dl...		<input type="checkbox"/>	In	Allow	System
dl...		<input type="checkbox"/>	In	Allow	C:\Windc
dl...	1723	<input type="checkbox"/>	Out	Allow	System
dl...		<input type="checkbox"/>	In	Allow	System
dl...	1701	<input type="checkbox"/>	Out	Allow	System
dl...		<input type="checkbox"/>	In	Allow	System
dl...		<input type="checkbox"/>	Out	Allow	C:\Windc
dl...	53	<input checked="" type="checkbox"/>	Out	Allow	C:\Windc
dl...		<input checked="" type="checkbox"/>	Out	Allow	C:\Windc
dl...	445	<input checked="" type="checkbox"/>	Out	Allow	System

Application	Port Range		Protocol	IP Address	Enabled
	Start	End			
lizz	6112	to 6112	Both	192.168.1.100	<input checked="" type="checkbox"/>
lizz2	6113	to 6113	Both	192.168.1.101	<input checked="" type="checkbox"/>
lizz3	6114	to 6114	Both	192.168.1.102	<input checked="" type="checkbox"/>
lizz4	6115	to 6115	Both	192.168.1.103	<input checked="" type="checkbox"/>
	0	to 0	Both	192.168.1.0	<input type="checkbox"/>
	0	to 0	Both	192.168.1.0	<input type="checkbox"/>

Challenges



- Key properties:**
- Clients don't know how their VMs are mapped in the network.
 - VMs being moved, which will have different network ports.
 - Clients can't easily view/query the FW policies related to their virtual networks.

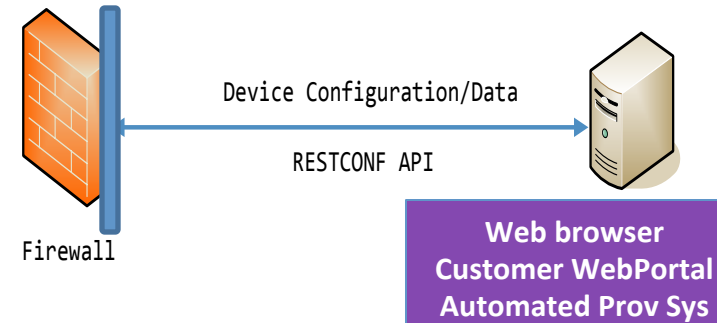
Common Functional components of FW

- **Functional components:**

- User authentication, user privilege control
- Policies, targets,
- Configuration, query, validation
- Logging, Reporting
- Maintenance methods
- ...

Interface to Clients:

Restful API:

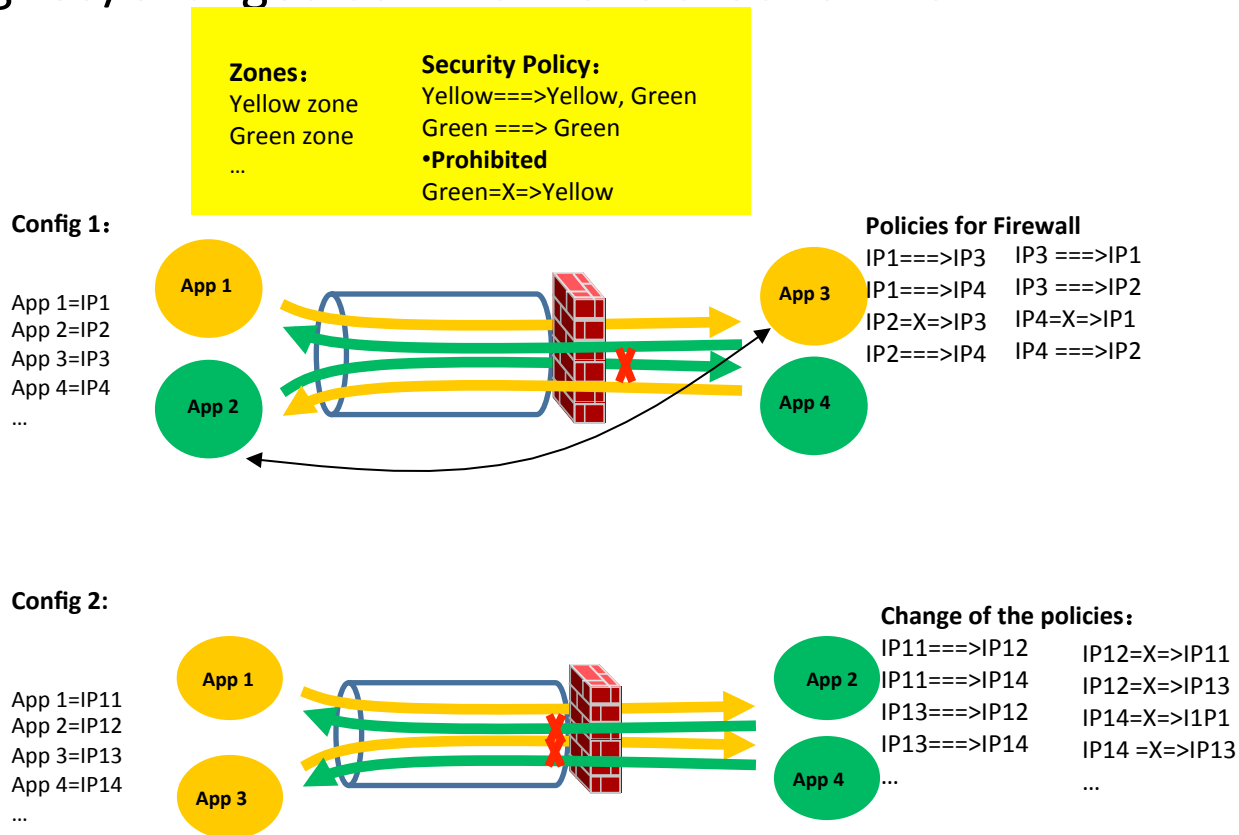


Web Portal

The screenshot shows a web portal interface for configuring a firewall rule. The title is 'New Inbound Rule Wizard'. The section is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' A 'Steps:' sidebar on the left lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main content area has two questions: 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP; and 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text input field for 'Specific local ports' contains '10933' and has an example below it: 'Example: 80, 443, 5000-5010'.

Goal: a common interface for client to specify desired network security functions

- Regardless if the policies are enforced by FW or other devices. Clients' policy stay the same regardless what IP/MAC address are assigned/changed as VMs move around DCs.



Security Functions under consideration:

- **The wide acceptance of security functions that are not running on customer premises. For example:**
 - Security as a Service:
https://cloudsecurityalliance.org/research/secaas/#_get-involved
 - Firewall as a Service :
<http://docs.openstack.org/admin-guide-cloud/content/fwaas.html>
 - Security has the sense of “long lasting services”. So we don’t have to deal with “On-Demand” oscillation issues.
- **Here are the network functions under consideration:**
 - **Firewall**
 - **IPS/IDS** (Intrusion detection system/ Intrusion prevention system)
 - **DDOS/AntiDoS**
 - **Access control/Authorization/Authentication**
 - **Secure Key management**

FW as a service: potential attributes

Attribute name	Type	Default Value	Description
id	uuid-str	generated	UUID for the firewall policy.
tenant_id	uuid-str	N/A	Owner of the firewall policy. Only admin users can specify a tenant_id other their own.
name	String	None	Human readable name for the firewall policy (255 characters limit).
description	String	None	Human readable description for the firewall policy (1024 characters limit).
shared	Boolean	False	When set to True makes this firewall policy visible to tenants other than its owner and can be used to associate with firewalls not owned by its tenant.
firewall_rules	List of uuid-str or None	None	This is an ordered list of firewall rule uids. The firewall applies the rules in the order in which they appear in this list.
audited	Boolean	False	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute is set to False and must be explicitly set to True through an update operation.

Security as a Service: Potential attributes

Table 7.29. Security group rules

Attribute name	Type	Default Value	Description
id	uuid-str	generated	UUID for the security group rule.
security_group_id	uuid-str or Integer	allocated by Networking	The security group to associate rule with.
direction	String	N/A	The direction the traffic is allow (ingress/egress) from a VM.
protocol	String	None	IP Protocol (icmp, tcp, udp, and so on).
port_range_min	Integer	None	Port at start of range
port_range_max	Integer	None	Port at end of range
ethertype	String	None	ethertype in L2 packet (IPv4, IPv6, and so on)
remote_ip_prefix	string (IP cidr)	None	CIDR for address range
remote_group_id	uuid-str or Integer	allocated by Networking or Compute	Source security group to apply to rule.
tenant_id	uuid-str	N/A	Owner of the security group rule. Only admin users can specify a tenant_id other than its own.

Relevant Industry initiatives:

- Firewall as a Service by OpenStack
 - OpenStack completed the Firewall as a Service project and specified the set of APIs for Firewall services:
http://docs.openstack.org/admin-guide-cloud/content/fwaas_api_abstractions.html
 - OpenStack has defined the APIs for managing Security Groups:
http://docs.openstack.org/admin-guide-cloud/content/securitygroup_api_abstractions.html
 - Attributes defined by OpenStack Firewall/Security as a Service will be the basis of the information model for the proposed work at VNFOD IETF initiative.
- Security as a Service by Cloud Security Alliance
 - SaaS by CSA is at the very initiate stage of defining the scope of work.