Bezpečnost ve virtualizovaném DC

SEC4 / L2

Tomáš Michaeli - Cisco
Speaker -
<table>
<thead>
<tr>
<th>DC Market</th>
<th>Cisco</th>
<th>VMware, Microsoft, Citrix, RedHat, Oracle</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Almost 65% of all datacenter workloads are virtualized</td>
<td>- Company extending direction from purely HW based appliance to SW based virtual service node</td>
<td>- VMware announced NXS</td>
</tr>
<tr>
<td>- Computing model has changed</td>
<td>- Easy service integration in virtual environment</td>
<td>- Windows 2012 released</td>
</tr>
<tr>
<td>- IT Service model has changed</td>
<td>- Cloud, automation</td>
<td>- Hypervisor market transforms to cloud market</td>
</tr>
<tr>
<td>- IT organizations expected to change</td>
<td>- SDN arena</td>
<td>- Competitors in one space, friends in other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cisco now partnering with Citrix</td>
</tr>
</tbody>
</table>
Data Center, Services, & Virtualization: It's so easy!

Just ask this 35 year old Administrator.
Agenda

- Architecture for virtualized services
- Understanding vPath
- Virtual Security Gateway overview
- Virtual ASA 1000V role in overall architecture
- Virtual Network Management Center overview
- VXLAN extend your cloud
- Summary
- Resources
Network team manages virtual & physical networks

- Modular Switch
  - Supervisor-1 (Active)
  - Supervisor-2 (StandBy)
  - Linecard-1
  - Linecard-2
  - Linecard-N

- Back Plane
- Network Admin

- Virtual Appliance
  - VSM-1 (active)
  - VSM-2 (standby)

- NX-OS Control Plane
- NX-OS Data Plane

- Server Admin
- Hypervisor
- VEM-1
- VEM-2
- VEM-N

Network team manages virtual & physical networks
Virtual Services Portfolio

### Virtual Appliance

- **ASA**
- **vWAAS**
- **VSG**
- **CRS**

- **VSM**: Virtual Supervisor Module
- **VSG**: Virtual Security Gateway
- **CRS 1000V**: Virtual Router
- **vWAAS**: Virtual WAAS
- **ASA 1000V**: Tenant-edge security

### Nexus 1010 / 1010X

Primary
- VSM
- NAM
- VSG

Secondary
- VSM
- NAM
- VSG

### Virtual Blades

- Virtual Supervisor Module (VSM)
- Network Analysis Module (NAM)
- Virtual Security Gateway (VSG)
- Data Center Network Manager (DCNM)

### L3 Connectivity

- **vPath**
  - Virtual service data-path
- **VXLAN**
  - Scalable Segmentation

- **VMware ESX**
- **Win 8 Hyper-V**
Virtual Services Node

Stand-alone VSN
Can be deployed with any virtual switch
Example: vWAAS

N1KV vPath integrated VSN
Integrates with N1KV port profile and virtual service datapath (vPath)
Example: vWAAS, VSG, ASA 1000V

VSN hosted on Nexus 1110 appliance
VSN can be stand-alone or vPath integrated
Example: VSG, NAM
n1000v# show port-profile name WebServers
port-profile WebServers
description:
status: enabled
capability uplink: no
system vlans:
port-group: WebServers
config attributes:
  switchport mode access
  switchport access vlan 110
  no shutdown
evaluated config attributes:
  switchport mode access
  switchport access vlan 110
  no shutdown
assigned interfaces:
  Veth10

Support Commands Include:
- Port management
- VLAN
- PVLAN
- Port-Channel
- ACL
- Netflow
- Port security
- QoS
Server Admin – Server configuration
Traffic monitoring for security or t-shooting purposes

<table>
<thead>
<tr>
<th>Port Profile</th>
<th>Port</th>
<th>Adapter</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Veth2</td>
<td>Veth15</td>
<td>Module 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>vmk0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>uplink</td>
<td>Po1</td>
<td>Po2</td>
<td>vmnic0</td>
</tr>
<tr>
<td></td>
<td>Eth8/1</td>
<td>vmnic1</td>
<td>prg-esx4.lab.prg.cisco.co</td>
</tr>
<tr>
<td></td>
<td>Eth8/2</td>
<td>vmnic1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Win2k8_AD</td>
<td>Veth9</td>
<td>Net Adapter 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veth65</td>
<td>Net Adapter 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veth68</td>
<td>Net Adapter 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Veth69</td>
<td>Net Adapter 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
sh int Veth9
Vethernet9 is up
Port description is Win2k8_PVT, Network Adapter 1
Hardware: Virtual, address: 0050.56aa.0009 (bia 0050.56aa.0009)
Owner is VM "Win2k8_PVT", adapter is Network Adapter 1
Active on module 8 VMware DVS port 928
Port-Profile is Win2k8_AD
Port mode is access
```

5 minute input rate 1712 bits/second, 1 packets/second
5 minute output rate 1864 bits/second, 1 packets/second

Rx 3235938 Input Packets 7133445 Unicast Packets 4603 Multicast Packets 78019 Broadcast Packets 340045398 Bytes...
Private VLAN for basic segmentation

Two ways to do Private VLAN

**Promiscuous Trunk**
The Nexus 1000V do the mapping from secondary vlan to primary vlan

**Trunk**
The Nexus 1000V rely on the upstream switch to do the mapping from secondary to primary vlan
VMs isolation with PVLAN or MAC ACL

- VM’s are Isolated or Community
- All VM’s talk to Promiscuous devices
- Only Primary VLAN needed outside
- MAC filter default-gateway

**With PVLAN**

port-profile type ethernet UPLINK

vmware port-group

switchport mode private-vlan trunk promiscuous

switchport private-vlan mapping trunk 60 61-63

switchport private-vlan trunk allowed vlan 2-5, 60-63

channel-group auto mode on mac-pinning

no shutdown

system vlan 2-5

state enabled

**With MAC ACL**

port-profile type vethernet access6

mac port access-group JustExternalHost in

mac access-list JustExternalHost

10 permit any 0022.1991.7e08 0000.0000.0000

20 deny any any
Understanding vPath and VXLAN
vPath 2.0 is now a part of N1kV

- Designed for virtualized network services
- VEM must be able to reach the L3 VSN
- Fast-Path Offload
- VSN on VXLAN
- Service chaining
- Proxy ARP required for L3
- Encapsulation Uplink MTU +96B
vPath service chain I. – Outside client to VM

1. Initial Packet Flow

2. L2/ L3

3. vPath Encap links

ASA inline Enforcement
vPath service chain II. – Outside client to VM

4. VSG Policy decision downloaded to VEM

5. vPath Encap links

Nexus 1000V Distributed Virtual Switch
vPath service chain III. – Outside client to VM

Nexus 1000V Distributed Virtual Switch

Policy offloaded to VEM

Traffic flow after first packet

vPath Encap links
vPath service chain I. – VM1 to VM2 inside VLAN

Nexus 1000V
Distributed Virtual Switch

ASA not in the path for the same Subnet VM to VM communication

vPath Encap links
vPath service chain II. – VM1 to VM2 inside VLAN
vPath service chain III. – VM1 to VM2 inside VLAN

Nexus 1000V Distributed Virtual Switch

vPath enforcing at VEM level and Policy offloaded from VSG to VEM

vPath Encap links
Example of VSG and ASA 1000V chain for tenant

- vservice node ASA1 type asa
  ip address 172.31.2.11
  adjacency I2 vlan 3770

- vservice node VSG1 type vsg
  ip address 10.10.11.202
  adjacency I3

- vservice path chain-VSG-ASA
  node VSG1 profile sp-web order 10
  node ASA1 profile sp-edge order 20

- port-profile type vethernet Tenant-1
  org root/Tenant-1
  vservice path chain-VSG-ASA

Defining the Service Node on Nexus 1000V
Chain the Service Nodes
Order is inside to outside
Enable the Service Chain Per Port-Profile
VXLAN: Reachability Across Subnet

- VM connectivity across L3 networks POD-to-POD, DC-to-DC
- VLAN indexes eXtension from 4k to 16M, IETF Standard Body
Tenant 1: virtual workloads protected by virtual firewall
Tenant 2: virtual workloads protected by physical firewall (via VXLAN GW)
Tenant 3: virtual & physical workloads in same L2 domain (via VXLAN GW)
VXLAN-VLAN Gateway example

VXLAN-Gateway

DB Server
Physical Workload

192.168.1.2

VLAN 33

192.168.1.1
Web - VM

VTEP:
10.20.20.51

VEM 1

192.168.1.2

192.168.1.3

Client- VM

VTEP:
10.20.20.21

VEM 2

VTEP:
10.20.20.61

VLAN 10000

VTEP: 10.20.20.21

The Internet

192.168.1.1

192.168.1.3

192.168.1.2

VLAN 33

192.168.1.2

DB Server
Physical Workload
Virtual Security Gateway overview
Virtual Security Gateway – Virtual Firewall for N1K

Virtual Security Gateway (VSG)

- Context Aware Security: VM context aware rules
- Zone-Based Control: Establish zones of trust
- Dynamic, Agile: Policies follow vMotion
- Best-in-Class Architecture: Efficient, fast, scale-out

Virtual Network Management Center (VNMC)

- Non-Disruptive Operations: Security team manages security
- Policy Based Administration: Central mgmt, scalable deployment, multi-tenancy
- Designed for Automation: XML API, security profiles
Deployment VSGs on Dedicated Host

- Dedicated Servers to host VSG Appliances
- Decouple Service from Compute Resources
- Easy to scale out with dedicated hosting of Service
Security Policy Building Block

Rule is analogous to an MCL; Policy is analogous to an ACL
VSG Policy – Rule Construct

<table>
<thead>
<tr>
<th>VM Attributes</th>
<th>Network Attributes</th>
<th>Operator</th>
<th>Network Attributes</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance Name</td>
<td>IP Address</td>
<td>eq</td>
<td>IP Address</td>
<td>eq</td>
</tr>
<tr>
<td>Guest OS full name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zone Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parent App Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Profile Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hypervisor Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>drop</td>
<td>member</td>
<td>192.168.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>permit</td>
<td>Not-member</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>reset</td>
<td>Contains</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>log</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VSG Policy – Zone based policy

<table>
<thead>
<tr>
<th>Zone</th>
<th>Attribute</th>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRNG</td>
<td>VM Name</td>
<td>Contains String</td>
<td>VT1-4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone=TRNG</td>
<td>ZONE=TRNG</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Any</td>
<td>Zone=TRNG</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Zone=TRNG</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
</tbody>
</table>
Use Case – Tier Server Zones

Permit Only Port 80 (HTTP) of Web Servers
Permit Only Port 22 (SSH) to Application Servers
Block All External Access to Database Servers

Policy — Content Hosting
# Use Case – Policy Rules with Zones

## Leveraging Zones in Rule Conditions

### Rule Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Source Condition</th>
<th>Destination Condition</th>
<th>Protocol</th>
<th>EtherType</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow-Web</td>
<td>Any</td>
<td>Network Port eq 80, vZone Name eq WebZone</td>
<td>eq TCP</td>
<td>Any</td>
<td>Permit, Log</td>
</tr>
<tr>
<td>Allow-SSH</td>
<td>Any</td>
<td>Network Port eq 22, vZone Name eq AppZone</td>
<td>eq TCP</td>
<td>Any</td>
<td>Permit, Log</td>
</tr>
<tr>
<td>Allow-Web-To-App</td>
<td>vZone Name eq WebZone</td>
<td>vZone Name eq AppZone</td>
<td>Any</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Allow-App-To-Web</td>
<td>vZone Name eq AppZone</td>
<td>vZone Name eq WebZone</td>
<td>Any</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Allow-App-To-DB</td>
<td>vZone Name eq AppZone</td>
<td>vZone Name eq DBZone</td>
<td>Any</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Allow-DB-To-App</td>
<td>vZone Name eq DBZone</td>
<td>vZone Name eq AppZone</td>
<td>Any</td>
<td>Any</td>
<td>Permit</td>
</tr>
<tr>
<td>Deny-Rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop, Log</td>
</tr>
</tbody>
</table>
VSG Policy Provisioning Logical Flow

- **Port Profile**
- **Protection**
- **Port Group**

Using VM/Network Attributes

- Create Rules-Based on Zones/Network Conditions
- Put Policy Set in the Security Profile

Assign Security Profile to Tenant VSG

Bind the Security Profile to Port Profile

Define Zones
Define Policy
Policy Set
Create Security Profile
Assign Tenant VSG

VNMC
Binding VSG Security Profile with N1kV Port-Profile

Security-Profile “SecureContractors” is attached to Port-Profile “contractor”
Virtual ASA 1000V role in overall architecture
Securing the tenant edge with Cisco ASA 1000V

- Proven Cisco security – physical and virtual consistency
- Collaborative security model
  - Cisco VSG for intra-tenant secure zones
  - Cisco ASA 1000V for tenant edge controls
- Transparent integration
  - Nexus 1000V Switch and vPath
- Scale flexibility to meet cloud demand
  - Multi-instance deployment for scale-out deployment across the data center
Virtual Form Factor Benefits

Efficient deployment as an ASA virtual machine

Deployed as you currently deploy or duplicate virtual machines and vApps

When the vApp or Tenant moves, the ASA 1000V can move with it

Example from VMware vCenter where Cisco ASA 1000V is part of the vApp it protects
Cisco ASA 1000V Solution Features and Capabilities

- Built using Cisco® ASA infrastructure
- Interoperability with Cisco VSG through service chaining
- VXLAN gateway
- Multi-tenant management Through Cisco VNMC
- IPsec VPN (site to site)
- NAT
- DHCP
- Default gateway
- Static routing
- Stateful inspection
- IP audit
- IP audit
Performance depends on the resources available for the Cisco ASA 1000V instance.

You can scale Cisco ASA 1000V by deploying additional instances.

### Per Instance of Cisco ASA 1000V

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum connections</td>
<td>200,000</td>
</tr>
<tr>
<td>Connections per second</td>
<td>10,000</td>
</tr>
<tr>
<td>VPN throughput</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>Maximum VPN tunnels</td>
<td>750</td>
</tr>
</tbody>
</table>
### Cisco ASA 1000V Scalability

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy rules per instance</td>
<td>4000</td>
</tr>
<tr>
<td>Minimum instances per tenant</td>
<td>1</td>
</tr>
<tr>
<td>Virtual machines secured per instance</td>
<td>512</td>
</tr>
<tr>
<td>Edge profiles per instance</td>
<td>32</td>
</tr>
<tr>
<td>Policies per policy set</td>
<td>256</td>
</tr>
</tbody>
</table>
Policies Enforcement with the ASA 1000V

1. Security Policy is attached to the Port-Profile
2. No vPath encapsulation for VM to VM communication in the same subnet
3. You can have different Port-Profile with different Security Profile for the same subnet
ASA 1000V DMZ use case

Two ASA 1000V Approach

Two Edge Firewalls one for inside subnet and other for DMZ subnet

No enforcement within Inside and DMZ VLAN

ASA 1000V and VSG Approach

Inside Security Profile and DMZ Security Profile addressing the security requirements for both Zones

Shared VLAN for both DMZ and Inside

Tenant A

PP-Inside (VLAN 200)

PP-DMZ (VLAN 400)

Inside

DMZ

PP- Port-Profile

SP- Security Profile

Tenant B

PP-Inside (VLAN 200)

PP-DMZ (VLAN 400)

Inside

DMZ
VNMC Overview
<table>
<thead>
<tr>
<th>ADSM</th>
<th>VNMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can configure both virtual and physical ASA from ASDM</td>
<td>Can manage both VSG and ASA 1000V</td>
</tr>
<tr>
<td>Provides real-time logs, statistics on VPN connections</td>
<td>Multitenant deployment</td>
</tr>
<tr>
<td>No VM attributes based policy configuration</td>
<td>Policies can be pre-configured for future deployment</td>
</tr>
<tr>
<td></td>
<td>Stateless model</td>
</tr>
<tr>
<td></td>
<td>VM attribute based policy for ASA 1000V</td>
</tr>
</tbody>
</table>
Virtual Network Management Center

Simple yet powerful network virtual services management

- Multi Tenant
  Different Customers, different needs
- Security Profiles
  Simple, policy based security configuration
- XML API
  3rd party integration ready
- Role Based Access Controls
  Different users, different privileges
- Nexus 1000V & vCenter
  Port profiles refer to security profiles
- Dynamic provisioning
  One stop configuration of network & security

Scalable
Stateless
Expandable
Partitionable
Integrated
Automated

VNMC GUI
Multitenant Org Structure

- Single Tenant can have up to 3 sub-levels of orgs
- Each sub-Level can have multiple orgs
- Overlapping Network Addresses across Tenants are supported
Administrative Roles

Tenant Level RBAC Access for Security Admin

1. VNMC Admin Roles
2. Tenant Level Access
<table>
<thead>
<tr>
<th>VNMC Systems Requirements</th>
<th>VSG System Requirements</th>
<th>ASA 1000V System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi 4.1 +</td>
<td>VMWare ESXi 4.0</td>
<td>VMware ESXi 4.1 +</td>
</tr>
<tr>
<td>vRAM: 3 GB</td>
<td>Nexus 1000V 1.4+</td>
<td>vRAM: 1.5 GB</td>
</tr>
<tr>
<td>vHDD: 25 GB</td>
<td>Virtual Network Management Center (VNMC)</td>
<td>vHDD: 1.5 GB</td>
</tr>
<tr>
<td>vCPU: 1</td>
<td>Licensing is based on per protected CPU socket (same as Nexus 1000V)</td>
<td>vCPU: 1 vCPU - 1 Ghz</td>
</tr>
<tr>
<td>Flash Player plug-in: version 11.2</td>
<td></td>
<td>vNIC: 4</td>
</tr>
<tr>
<td>Firewall ports requiring access</td>
<td></td>
<td>Licensing is based on per protected CPU socket (same as Nexus 1000V)</td>
</tr>
<tr>
<td>80 (HTTP/TCP), 443 (HTTPS), 843 (TCP)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Resume

Shift in Virtual Network Services strategy
VXLAN extends L2 boundaries and extend VLAN IDs for vCD
vPath traffic interception without topology change
Nexus 1000V is foundation for virtual services
Virtual Security Gateway zone based firewall between VMs
Virtual ASA is edge firewall for traffic entering/leaving tenants
Virtual WAAS easy traffic optimization in virtual environment
Upcoming Public Webcasts, Spring 2012

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/10</td>
<td>Cloud Security with ASA 1000V and Virtual Security Gateway v2.1 (VSG)</td>
<td></td>
</tr>
<tr>
<td>4/17</td>
<td>Secure Hybrid Cloud solution with Nexus 1000V InterCloud &amp; VNMC InterCloud</td>
<td></td>
</tr>
<tr>
<td>4/24</td>
<td>Nexus 1100 for Cloud Network Services: New Services &amp; Ecosystem</td>
<td></td>
</tr>
<tr>
<td>5/1</td>
<td>Cloud Networking Services: vNAM and vWAAS</td>
<td></td>
</tr>
<tr>
<td>5/8</td>
<td>Virtualized Multiservice Data Center (VMDC) solution with Cloud Networking Services</td>
<td></td>
</tr>
<tr>
<td>5/15</td>
<td>Nexus 1000V for KVM (with OpenStack and VXLAN)</td>
<td></td>
</tr>
</tbody>
</table>

Webinar Link: [www.cisco.com/go/1000vcommunity](http://www.cisco.com/go/1000vcommunity)
Hands on for virtual networking specialists

- Hands-on labs available for Cisco® ASA 1000V, Cisco VSG, and Cisco Nexus® 1000V in Cisco Cloud Lab
  
  https://cloudlab.cisco.com

- Open to all Cisco employees

- Customers/Partners require sponsorship from account team for access via CCO LoginID

- Extended duration lab licenses for 1000V and VSG are available upon request
Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v sále LEO v 17:45 – 18:30

e-mail: connect-cz@cisco.com
Prosíme, ohodnoťte tuto přednášku.
Děkujeme za pozornost.