Data Center Security Challenges and Solutions

Automated Security for Today’s Dynamic Data Centers

Mohammad AlYousef
Sr. Systems Engineer
Security Functions in the Data Center

- Traditional Firewall Functions
- VPN Functions
- Context Aware Functions
- IPS Functions
- Web Functions
Key Trends for Security in the Data Center

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
Key Trends for Security in the **Data Center**

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
<table>
<thead>
<tr>
<th>Data Center Scale</th>
<th>TOTAL THROUGHPUT</th>
<th>CONCURRENT CONNECTIONS</th>
<th>CONNECTIONS / SEC</th>
<th>POWER &amp; SPACE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

©2013 Cisco and/or its affiliates. All rights reserved.
Key Trends for Security in the Data Center

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
## Network Integrated Clustering & Resiliency

### Technology

- Integration with VSS, vPC and Fabric Path
- Consistent Scaling Factor
- Pay as You Grow
- FW, VPN, IPS Services

### Benefit

- Ease of Deployment Solves Asymmetric Traffic
- Linear, Predictable Performance Increase
- Only Buy What You Need
- Compliance and Security

---

Integration with DC Switches

Clustered Security Services Using N+1 HA

---

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Key Trends for Security in the Data Center

**Scale**: Need for policy enforcement for high speed networks

**Resiliency**: High availability is imperative for applications

**Expanded Deployment Options**: Policy enforcement on inter-DC traffic

**Segmentation**: Policy between specific groups, users, or applications

**Contextual Analysis**: Global and local threat correlation

**Virtualization**: Security for east-west traffic in multi-hypervisor environments
Symmetric Traffic Patterns in the Data Center

Inside Network

Client

Security Services Cluster

Server

Outside Network
Symmetric Traffic Patterns in the Data Center

Inside Network

Client

Security Services Cluster

Outside Network

Server
Symmetric Traffic Patterns in the **Data Center**
Asymmetric Traffic Patterns in the Data Center

Security Services Cluster

Client → Director → Forwarder → Owner → Server

Inside Network

Outside Network
Asymmetric Traffic Patterns in the Data Center
EXPANDING SECURITY BETWEEN DATA CENTERS

Use Cases

- Disaster Recovery: Power outage, catastrophic failure
- Follow the sun operations: Optimization of resources
- Dynamic Load Distribution: Dealing with traffic bursts
# EXPANDING SECURITY BETWEEN DATA CENTERS

## Infrastructure Demands

<table>
<thead>
<tr>
<th>Simplicity</th>
<th>Traditional Approach</th>
<th>Optimized Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over-provisioned HW</td>
<td>Workload mobility</td>
<td>Workload mobility</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Low Latency</th>
<th>Manual traffic engineering</th>
<th>Optimize traffic flows to minimize latency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static, external stateless LB</td>
<td>Security state maintained with application mobility via CCL</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>High Scale</th>
<th>Siloed HA at different sites – no sharing of info</th>
<th>Persistent security HA across DC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siloed HA at different sites – no sharing of info</td>
<td>Persistent security HA across DC</td>
<td></td>
</tr>
</tbody>
</table>

- **Simplicity**: Over-provisioned HW
- **Low Latency**: Manual traffic engineering
- **High Scale**: Static, external stateless LB
- **High Availability**: Siloed HA at different sites – no sharing of info

## Traditional Approach

- Simplicity:
  - Over-provisioned HW
- Low Latency:
  - Manual traffic engineering
- High Scale:
  - Static, external stateless LB
- High Availability:
  - Siloed HA at different sites – no sharing of info

## Optimized Approach

- Workload mobility
- Optimize traffic flows to minimize latency
- Security state maintained with application mobility via CCL
- Persistent security HA across DC
Key Trends for Security in the Data Center

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
Unified Context & Network Control – TrustSec +ASA

TrustSec Overview

TrustSec lets you define policy in meaningful business terms

Business Policy

<table>
<thead>
<tr>
<th>Destination</th>
<th>HR Database</th>
<th>Prod HRMS</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec BYOD</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Exec PC</td>
<td>✗</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>Prod HRMS</td>
<td>✔</td>
<td>✔</td>
<td>✗</td>
</tr>
<tr>
<td>HR Database</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Distributed Enforcement throughout Network

Switch | Router | DC FW | DC Switch
Key Trends for Security in the **Data Center**

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
Turning Big Data into Threat Intelligence

SECURITY SENSOR BASE
Broadest range of threat & vulnerability data sources

THREAT ANALYTICS
Global and local correlation through analytics and human intelligence

INTELLIGENCE DELIVERED
Contextual Policy with Distributed Enforcement

100TB
Security Intelligence

13B
Web Requests

93B
Daily Email Messages

150M
Deployed Endpoints

14M
Deployed Access Gateways

1.6M
Deployed Security Devices

100TB Security Intelligence

13B Web Requests

93B Daily Email Messages

150M Deployed Endpoints

14M Deployed Access Gateways

1.6M Deployed Security Devices

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Key Trends for Security in the *Data Center*

- **Scale**: Need for policy enforcement for high speed networks
- **Resiliency**: High availability is imperative for applications
- **Expanded Deployment Options**: Policy enforcement on inter-DC traffic
- **Segmentation**: Policy between specific groups, users, or applications
- **Contextual Analysis**: Global and local threat correlation
- **Virtualization**: Security for east-west traffic in multi-hypervisor environments
TRAFFIC TRENDS IN DATA CENTER

- East – West Traffic: 76%
- North – South Traffic: 17%
- Inter-DC Traffic: 7%

Source: Cisco Global Cloud Index 2012 by destination
TRADITIONAL APPROACH TO TRAFFIC TRENDS

Infrastructure Demands

Traditional Approach

- Insert East-West Services | Traffic Hairpinning
- Need for Scale | Over-provision HW
- Diverse Users/Devices | Rules Explosion
- Rapid Provisioning | Manual & Fragmented
APPLICATION TRENDS IN DATA CENTER

DYNAMIC WORKLOADS
- Dynamic Instantiation/Removal

HETEROGENEOUS IMPLEMENTATION
- Physical & Virtual

DISTRIBUTED DEPLOYMENTS
- On-Demand Scaling

INFRASTRUCTURE INDEPENDENT
- Transparent to Underlying Network

CLOUD-AWARE
- Migration across public/private clouds

Instantiate new VM
Decommission existing VM
Migrate existing VM
The adoption rate of server virtualization will reach 21.3% of total servers in 2016.

GARTNER
APPLICATION TRENDS IN DATA CENTER

DYNAMIC WORKLOADS
- Dynamic Instantiation/Removal

HETEROGENEOUS IMPLEMENTATION
- Physical & Virtual

DISTRIBUTED DEPLOYMENTS
- On-Demand Scaling

INFRASTRUCTURE INDEPENDENT
- Transparent to Underlying Network

CLOUD-AWARE
- Migration across public/private clouds

New Applications, Devices & Users

New Applications, Devices & Users
APPLICATION TRENDS IN DATA CENTER

DYNAMIC WORKLOADS
- Dynamic Instantiation/Removal

HETEROGENEOUS IMPLEMENTATION
- Physical & Virtual

DISTRIBUTED DEPLOYMENTS
- On-Demand Scaling

INFRASTRUCTURE INDEPENDENT
- Transparent to Underlying Network

CLOUD-AWARE
- Migration across public/private clouds

Dynamically Shared Resource Pools
- oversubscribed
- underutilized
- optimized

Siloed Resources
Shared Resource Pools
APPLICATION TRENDS IN DATA CENTER

DYNAMIC WORKLOADS
- Dynamic Instantiation/Removal

HETEROGENEOUS IMPLEMENTATION
- Physical & Virtual

DISTRIBUTED DEPLOYMENTS
- On-Demand Scaling

INFRASTRUCTURE INDEPENDENT
- Transparent to Underlying Network

CLOUD-AWARE
- Migration across public/private clouds

By 2016, 66% of all workloads will be processed in the cloud
CISCO GLOBAL CLOUD INDEX

Secure Multi-tenant

Inter-DC
Private - Public
Public

Migration across public/private clouds
KEY REQUIREMENTS TO ADDRESS DC TRENDS

- **Simplified Provisioning**
  - Dynamic workloads
  - Centralized Management
  - Physical/Virtual agnostic

- **Dynamic Scaling**
  - Dynamic On-Demand
  - Physical + Virtual
  - Location independent

- **Centralized Management**
  - Centralized policy for network & security
  - Rapid instantiation based on resource availability

- **Automated Policy Management**
  - Dynamic ACL insertion / removal

- **Open Architecture**
  - Hypervisor agnostic
  - vSwitch compatible
  - Programmable API
  - Multi-tenant aware
  - Application aware
APPLICATION-CENTRIC INFRASTRUCTURE

ENABLING APPLICATION VELOCITY – ANY APPLICATION, ANYWHERE

Physical Networking
Nexus 7K
Nexus 2K

Hypervisors and Virtual Networking
vmware
redhat
Xen

Compute

L4–L7 Services

Storage

Multi DC WAN and Cloud
Integrated WAN Edge

Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014
Cisco Connect, Riyadh, Saudi Arabia, April 29-30, 2014

CISCO’S APPLICATION CENTRIC INFRASTRUCTURE SECURITY SOLUTION

- Transparent Integration of Security into Cisco’s Application Centric Infrastructure
- Centralized Infrastructure with Automated Security Policy Management
- Elastic Scalability across Virtual and Physical Environments
ACI SECURITY SOLUTION STARTS WITH CISCO ASA

VIRTUAL

ASAv
• Full ASA Feature Set
• Hypervisor Independent
• Virtual Switch Agnostic
• Dynamic Scalability

PHYSICAL

ASA 5585-X
16 Way Clustering with State Synchronization
Scalable to 640Gbps

ASAv on VMWare – Available in Beta Today – Ask your SE
CISCO SECURITY INTEGRATED INTO ACI

PROVISIONING
- Simplified Service Chaining
- Dynamic Policy Management
- Rapid Instantiation

PERFORMANCE
- On Demand Scalability
- Increased Clustering Size
- Multi-Site Clustering

PROTECTION
- Integrated Security and Consistent Policy Enforcement (Physical & Virtual)
- Active Monitoring & Comprehensive Diagnostics for Threat Mitigation
The Network and Security: Synergies Drive Value

- Consistent, End-to-end Security Policy Enforcement
- Data Center Service Clustering Delivers Unmatched Scale
- Mobility and BYOD Accelerator / Enabler
- Automated Network Re-direction
- Rich Data Sets Accelerate Threat Detection
- Scales Enforcement
- Network
- Security
- Aggregates Unique Context
- Accelerates Detection