What You Make Possible
Firewall Architectures
BRKSEC-2021
Related Sessions

- BRKSEC - 1006v – Network Segmentation For Security
- BRKSEC – 2020 – Firewall Deployment
- BRKSEC – 2205 – Security and Virtualization in the Data Center
- BRKSEC – 3020 – Troubleshooting Firewalls
- BRKSEC – 3021 – Maximizing Firewall Performance
- BRKVIR – 2011 – Deploying Services in a Virtualized Environment
Session Info and Housekeeping

- This is a new session for 2012 based upon previous years feedback and is closely tied to BRKSEC-2205 (Securing the Virtualized Data Center)
- We will use a case study format to highlight an architecture that highlights both physical and virtual firewalls
- Pros and cons of each architecture will be discussed
- New for Cisco Live 2012—90 minute sessions so we will move fast 😊
- Please note: this session discusses products and features that are not currently shipping
- I will be available after the session to answer questions
- This session does not cover IOS firewall or the Firewall Services Module (FWSM)
Agenda

- Introduction to ACME
- Phase 1 – Data Center Refresh
- Phase 2 – Securing Private Cloud
- Phase 3 – Enhancing Visibility in the Cloud
- Phase 4 – Firewall Clustering
- Phase 5 – Application Firewall at Internet Edge
- Summary
- Q & A
ACME Case Study
Introduction to ACME Incorporated

- Fictional company based upon real discussions with real customers
- ACME leadership want to enhance the current network in order to rapidly deploy new technologies as they become available
- ACME also wants to combine virtualized application services between business units
- This application delivery creates an immediate need for more compute
- The physical server infrastructure will be augmented by a migration to virtualization technologies and private cloud
- ACME will continue to utilize existing segmentation technologies, the basic building blocks being VRFs, VDCs and VLANs
ACME’s High Level Design and Project Plan

- ACME’s leadership has approved a far-reaching plan to enhance the existing network infrastructure over the coming year:

- This plan is broken into five phases:
  1. Update the core network infrastructure, optimize path redundancy
  2. Begin migration of physical server infrastructure to virtualized infrastructure
  3. Build a network that will support private cloud with multi tenancy
  4. Migrate to firewall clustering
  5. Improve application visibility at the edge

- The underlying requirement for network expansion is that the ACME Inc. security policy must scale in proportion and be ubiquitous regardless of access methodology (wired, wireless, VPN, etc)
ACME’s security team has three requirements for the new network architecture:

1. Security policy must scale to the network infrastructure
2. Must meet or exceed regulatory compliance requirements in all phases
3. All security devices must be deployed with high availability (HA)
The ACME Network Today

- ACME is divided into four blocks:
  1. Campus
  2. Data Center
  3. DMZ
  4. Internet Edge

- Network requirement is dual-homed for path redundancy where possible

- L3 routed core (BGP)
ACME Phase 1

Upgrade the Network Infrastructure for Regulatory Compliance
ACME Phase 1 – Repurpose Older Gear

- The network upgrade included a migration from older Catalyst 6500 switches to the Nexus 7000 for the ACME data center.
- Rather than retire the older Catalyst 6500s they decided to repurpose them for the campus block as services chassis.
- ACME installs ASA SMs in order to take advantage that most of their infrastructure is segmented into VLANs.
- Where necessary VRFs map to VLANs for more extensive segmentation and path isolation.
- This eases the migration for a future deployment of Security Group Tags (SGT) and 802.1x that will facilitate an identity based security policy (AD users and groups).

ASA SM Blade Insertion in HA mode

- ASA SM has no physical interfaces; uses VLANs in Supervisor module as network "interfaces"
- Easy migration path for FWSM installs
- Policy is applied per-VLAN
- Popular in multi-tenant environments
- Runs ASA code base, IPv6 support
ACME Phase 1 Requirements

- Regulatory compliance dictates that there must be **stateful inspection** for flows to and from the data center block which contains the server farms.
- This will require a firewall to be placed in between the L3 point-to-point links that connect to the ACME routed core.

**Option 1**: Deploy a L3 firewall that supports BGP and modify IP scheme.

**Option 2**: Deploy a L2 firewall (transparent mode).

- Both options support HA as per the security team requirement.
- Option 2 is the better choice for ACME today.
What is a Transparent mode Firewall?

- Transparent Firewall (L2) mode provides an option in traditional L3 environments where existing services can’t be sent through the firewall
- Very popular architecture in data center environments
- In L2 mode:
  - Routing protocols can establish adjacencies through the firewall
  - Protocols such as HSRP, VRRP, GLBP can pass
  - Multicast streams can traverse the firewall
  - Non-IP traffic can be allowed (IPX, MPLS, BPDUs)
  - Allows for three forwarding interfaces, inside and outside and DMZ
  - NO dynamic routing protocol support or VPN support
  - Specific design requirements, reference Configuration Guide for details
The ACME Network Revisited

ACME Data Center

L3 Routed Core

Fully Meshed BGP

Network Edge

ISP-A

ISP-B
ACME Phase 1 Deployment Requirement

- These are L3 point-to-point links that connect to the ACME routed core
- ACME requires a L2 firewall between L3 links
- Firewall is processing at L2 (VLANs) while L3 services are unaffected if permitted by firewall access control list (ACL)
ACME L2 Deployment Logical View
Case Study: ACME Network Packet Flow (Detail View)

- **Inside VLAN 100**: 192.168.0.1 /29
- **Outside VLAN 100**: 192.168.0.3 /29
- **SVI VLAN 100**: 192.168.0.1 /29
- **Inside VLAN 100 (outside)**
- **Outside VLAN 200**: 192.168.0.2 /29
- **Active FW int BVI 1**: 192.168.0.5 /29
- **HA Interconnects**: Green lines are trunks
- **SVI VLAN 100 (outside)**
- **L3 interface**: 192.168.0.2 /29
- **L3 interface**: 192.168.0.4 /29
ACME Phase 1 Physical View

- Trunk connections to the Nexus 7000s
- Two HA connections for state and keepalives (dashed lines)
- L3 traffic is unaffected if permitted by firewall ACL
- Firewalls only see VLANs at L2
- This is achieved using subinterfaces on the firewall
- STP will block one of the firewall links
Preserving Path Redundancy

- ACME’s network team requires that any network device in the data center must be dual-homed for critical path redundancy
- Security team is challenged with how to deploy L2 firewall in a manner that meets these requirements
- A possible solution is configuring Virtual Port Channels (VPC) on the ASA firewall
- Port channel support was added to the ASA in 8.4 (2011)
- Leveraging this feature gives ACME uptime benefits like other devices in the data center
- VPC offers two forwarding paths and removes spanning-tree requirement
- In the event of a single link failure there is no packet loss
Virtual Port Channel (VPC) Explained

- A virtual port channel is port channel between more than two devices
- VPC was created to solve two inherent network problems: Spanning-tree recalculation times and unused capacity in redundant L2 uplinks (due to STP blocks)*
- Supported in Nexus OS

- VPC Design Guide:

* For a good discussion on VPC basics see John Herbert's blog here:
ACME Phase 1 Complete

- Trunk connections to the Nexus 7000s
- Links from firewalls are Virtual Port Channels (VPC)
- Allows for maximum dual uplink resiliency for data path
- Active/Standby or Active/Active firewall HA for data plane
- Dashed lines are for HA only
ACME Phase 1 Summary

- ACME reallocated older 6500s as services chassis for provisioning security services via the ASA SMs deployed in HA
- ACME installed two ASA 5585s in L2 mode to protect the data center server farms for regulatory compliance
- L2 firewalls minimize upper layer protocol disruption (RP, voice, etc)
- ACME will have to design accordingly to not exceed 8 bridge-group limit of L2 firewall; otherwise multi-mode (virtual) firewall is an option
- These ASAs were deployed in HA for firewall redundancy as well as VPC for path redundancy to the Nexus 7000 switch infrastructure
- This gives ACME a very resilient firewall in the data center where uptime is critical
- Time to move to Phase 2……
ACME Phase 2
Foundation for Private Cloud
ACME Phase 2: Foundation for Private Cloud

- Like many companies, ACME has made a commitment to augment/migrate their existing physical server infrastructure to a virtualized one.
- Virtualization meets their requirements for application service agility.
- The challenge for ACME’s security team is to maintain security controls on a rapidly expanding infrastructure.
- Their security policy must be flexible enough to be enforced in both the bare metal appliance infrastructure as well as the virtualization layer.
ACME Phase 2 Security Requirements

- Security policy must scale with network infrastructure growth
- ACME builds tiered zones of virtual servers that have a common purpose (web, database, application, etc.)
- Regulatory compliance dictates that stateful access controls must exist when data enters a zone
- ACME needs a scalable firewall option
What are North-South and East-West Flows?

- North-South (N-S) flows are typically flows to and from Access layer to Aggregation Layer and Core.

- East-West (E-W) flows typically stay either within a zone or between zones and often server to server traffic.
Option 1: Utilize Existing DC Firewalls

- ACME recently invested in two new firewalls for the data center.
- One option is to send all N-S flows to the new firewalls for inspection.
- East-West flows inside each zone would **not** be inspected unless there was L2 separation.
- Does not provide any access controls for hosts that are L2 adjacent.
Option 1 Benefits and Challenges

- Meets security and network requirements, all flows leaving a zone will have to pass through a security enforcement point (firewall)
- Flows inside the zone are not inspected (L2 adjacent)
- Max concurrent connections limit becomes critical for the firewall
- Possible solution for a smaller topology but will be challenged to scale
- L2 firewalls may exhaust bridge-groups
- Inefficient traffic flow if most flows are zone to zone
- Larger capacity firewalls might be required depending on resources consumed by zone traffic
- Does not address ACME preference for virtual machine mobility
Option 2: Dedicated Zone FW Appliances

- Another option is to add new firewall appliances into the access layer
- Still meets security and network requirements
- Firewalls can be deployed in L3 or L2 mode
- Increased OPEX overhead
- Won’t scale if zone growth is rapid and consistent
- Might not address the issue of virtual mobility (Vmotion)
Option 3 – Deploy the ASA 1000V

- ASA1000V is a software-only version of an ASA appliance
- Runs ASA codebase in a virtual machine in L3 mode only
- ASA1000V for each pod, acts as edge firewall
- Scales with virtual infrastructure
- Addresses the virtual mobility problem
- Can be deployed in active/standby HA
- Requires N1KV for vPath
Option 3 Benefits and Challenges

- ASA 1000V is a new construct of an ASA in a virtual machine
- Requires the Nexus 1000V for deployment, licensed per CPU socket
- Designed as an L3 edge firewall for cloud environments
- Managed via ASDM or Virtual Network Management Center (VNMC)
- No hardware acceleration, software only
- Since ASA1000V utilizes N1KV constructs packet flow is optimized and does not require looping traffic in and out like a traditional virtual appliance due to vPath architecture
- Increased network complexity as a tradeoff to scalability and mobility
- Has a minimal feature set of an ASA appliance
ASA 1000V Unsupported Features

- Remote access VPN (does support IPSEC P2P VPN)
- Unified Communication Feature Set
- Botnet Traffic Filter (BTF)
- WCCP
- Routing protocols
- Netflow (but N1KV supports this)
- Multi context mode (virtual firewall)
- No HA active-active support
Phase 2 Summary

- ACME successfully deployed a massive expansion of their resources for compute through a migration to virtualization.
- There are at least three options for meeting their new security requirement of inspecting all traffic sourced or destined for a data center zone.
- This requirement is phased for their future foundation in private cloud.
- Firewalls can be either physical or virtual with each having specific benefits and challenges.
- The best choice is one that meets the security and network requirements and matches the operational flow of the organization.
- ASA 1000V is not a replacement for ASA firewall appliances!
Nexus 1000V Basics
Architecture, Port Profiles and vPath
Nexus 1000V Architecture

Virtual Supervisor Module (VSM)
- CLI interface into the Nexus 1000V
- Leverages NX-OS
- Controls multiple VEMs as a single network device
- Not in data path!

Virtual Ethernet Module (VEM)
- Replaces Vmware DVS
- Enables advanced switching capability on the hypervisor
- Provides each VM with dedicated “switch ports”

Network Admin

Modular Switch

Back Plane
- Supervisor-1
- Supervisor-2
- Linecard-1
- Linecard-2
- Linecard-N

Virtual Appliance
- VSM1
- VSM2

VEM-1
- Hypervisor
- Server Admin

VEM-2
- Hypervisor
- Server Admin

VEM-N
- Hypervisor
- Server Admin
Nexus 1000V Port Profiles

Nexus 1000V supports:
- ACLs
- Quality of Service (QoS)
- PVLANs
- Port channels
- SPAN ports

* For more detail, see BRKVIR-3013 Deploying and Troubleshooting the Nexus 1000V
What is vPath?

- vPath is the forwarding “brains” built into the Virtual Ethernet Module (VEM) of the Nexus 1000V
- It is an encapsulation that tags flows based upon attributes
- It has two main functions:
  1. Intelligent traffic steering
  2. Offload processing from virtual service nodes (VSN) to VEM
- vPath allows processing to be offloaded to Hypervisor for performance
- Currently only supported on VMWare today with future support for Hyper-V and others
- vPath is cornerstone for Cisco’s VSN delivery
ACME Phase 3
Enhanced Visibility and Control in the Private Cloud
ACME Phase 3: Preparing for Private Cloud

- Now that the virtualized compute and infrastructure build out is complete, ACME has determined that a private cloud offering could expand their business portfolio.
- In order to meet their projected growth, ACME will have to continue expand their data center.
- This opens up a new security requirement since different entities will be accessing zone services where there is currently no trust relationship.
- The new security standard requires that hosts and services inside a zone must be segmented in such a manner that all access is inspected between zone members.
- This is required regardless of existing L2 or L3 boundaries.
ACME Phase 3 Detailed View

Web Zone

Database Zone

App Zone
ACME Phase 3 Packet Flow

- This requirement adds a tremendous challenge as it essentially mandates that each VM be on an “island” for security purposes.
- ACME can silo certain applications and services for ease of administration.
- But this is still a challenge to push security down to this layer due to scalability requirements of network team.
ACME Phase 3 Option 1: Private VLANs

- Private VLANs (PVLAN) are used for L2 isolation and are supported in most Cisco switches.
- Use isolated and community ports with PVLAN.
- Packets are sent to promiscuous ports for routing and security inspection.
- Meets security requirement of L2 isolation but adds complexity.
- Scalability concerns, VLAN dependency.
Phase 3 Option 2: Virtual Security Gateway

- VSG is a L2 firewall that leverages vPath and port profiles created on the Nexus 1000V
- It enforces security policy via zones regardless of L2/L3 adjacencies
- Policy is built on standard 5 tuple (src/dst IP, protocol) or virtual machine attributes
- Allows security policy to be embedded at the hypervisor level
### VM Attributes Used by VSG (Partial List)

<table>
<thead>
<tr>
<th>Name</th>
<th>Meaning</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm.name</td>
<td>Name of this VM</td>
<td>vCenter</td>
</tr>
<tr>
<td>vm.host-name</td>
<td>Name of this ESX-host</td>
<td>vCenter</td>
</tr>
<tr>
<td>vm.os-fullname</td>
<td>Name of guest OS</td>
<td>vCenter</td>
</tr>
<tr>
<td>vm.vapp-name</td>
<td>Name of the associated vApp</td>
<td>vCenter</td>
</tr>
<tr>
<td>vm.cluster-name</td>
<td>Name of the cluster</td>
<td>vCenter</td>
</tr>
<tr>
<td>vm.portprofile-name</td>
<td>Name of the port-profile</td>
<td>Port-profile</td>
</tr>
</tbody>
</table>
VNMC Policy Zone Inspection

Virtual Network Management Center

Security Policies
Device Policies
Capabilities
Diagnostics

Firewall Policy
-Root
-Object Groups

Policies
- Policy Sets
- Zones
- CFC
- Object Groups
- Policies
- Security Profiles
- Security Profile Dictionary

Deny_Interzone_traffic

Add Rule | Up | Down | Destination Condition | Protocol | Ethertype | Action
---|---|---|---|---|---|---
 Permit_Finance | Zone Name eq Finance | Zone Name eq Finance | Any | Any | Permit
 Permit_HR | Zone Name eq HR | Zone Name eq HR | Any | Any | Permit
 Deny_HR_to_FI | Zone Name eq HR | Zone Name eq Finance | Any | Any | Drop, Log
 Deny_Finance_to_HR | Zone Name eq Finance | Zone Name eq Finance | Any | Any | Drop, Log
 Permit_ALL | Any | Any | Any | Any | Permit
VNMC Security Policy per Zone
Phase 3 Option 2 Benefits and Challenges

- VSG is software only, runs as a virtual firewall at L2
- Zones are building blocks for policy
- One or more VSGs deployed per tenant (do not share VSGs among tenants)
- VNMC manages both ASA1000V policy and VSG policies and is built for multi-tenant environments
- VSG can be deployed in Active/Standby for HA
- Policy follows virtual machine regardless of physical location
- Rapidly deployed via automation and orchestration software (OVA)
- Virtual Security Gateway requires Nexus 1000V for deployment
- Increases complexity due to distributed VSwitch requirement
# ASA1000V and VSG Compared

<table>
<thead>
<tr>
<th>ASA 1000V (Edge)</th>
<th>Virtual Security Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>L3 routed mode only</td>
<td>L2 mode (transparent)</td>
</tr>
<tr>
<td>Static routes only</td>
<td>No routing</td>
</tr>
<tr>
<td>DHCP server and client support</td>
<td>No DHCP support</td>
</tr>
<tr>
<td>Supports site-to-site IPSEC</td>
<td>No IPSEC support</td>
</tr>
<tr>
<td>Managed by ASDM and VNMC</td>
<td>Managed by VNMC only</td>
</tr>
<tr>
<td>Uses ASA code, CLI, SSH</td>
<td>Minimal config via CLI, SSH</td>
</tr>
<tr>
<td>Installed via OVA</td>
<td>Installed via OVA</td>
</tr>
<tr>
<td>Nexus 1000V vPath support</td>
<td>Nexus 1000V vPath support</td>
</tr>
</tbody>
</table>
ACME Phase 4

Firewall Clustering
ACME Phase 4: Firewall Clustering

- In order to prepare for a future data center expansion, ACME’s network team has opted to migrate from the traditional Cisco firewall Active-Standby model to a clustered model.
- This will allow them to have all firewalls actively forwarding and participating in inspection (unlike Active-Standby).
- This is a new feature in the ASA 9.0 code which as of June 2012 has not been released yet (expected release in late July/August).
- Since it involves a major change in how Cisco firewalls can be placed in the data center it is addressed in this session.
- Clustering is a licensed feature and only supported on the 5580 and 5585 models.
ASA Clustering Design Guidelines

- Up to 8 ASAs are supported in a cluster (minimum of two) and all must be the same model and DRAM (only flash memory can differ)
- All cluster units must share same software except during a hitless upgrade (e.g. 9.0(0)1 to 9.0(0)3)
- Approximate maximum cluster throughput is ~ 70% of combined throughput and connections of units in the cluster
- Cluster will have one master and syncs configuration with other members
- Supported in both routed (L3) and transparent (L2) firewall modes
- Requires at least one cluster control interface for cluster control plane
- Cluster control links must be sized properly to accept a load that is equal to or greater than the cluster throughput
ASA Clustering Best Practices – Control Plane

- Cluster control links must be sized accordingly (e.g. 10GE interfaces)
- Recommended to use a local port-channel on each ASA for link redundancy and aggregation
- Do NOT use a spanned port-channel for cluster control links
- Could also use ASA interface redundancy which supports up to 8 pairs of interfaces in an active-passive mode
ASA Clustering Best Practices – Data Plane

- ASA clustering relies upon stateless load balancing
- Could also use a load balancer if stateful LB was required
- Recommended method is to use a spanned port-channel to a switch for ingress and egress connections
- BP is to use a symmetrical hashing algorithm like src-dest IP (the default)
- Could also use Policy Based Routing (PBR) or Equal Cost Multi-Path (ECMP); use both with Object Tracking
- Both the latter two methods are only supported in routed (L3) mode on the firewall
ASA Features Unsupported with Clustering

- SSL and IPSEC remote access VPN (Site to Site VPN is supported)
- Legacy VPN load balancing is not supported for S2S VPNs
- Botnet Traffic Filter (BTF)
- DHCP Client, Server and Relay
- VPN Load Balancing
- Unified Communications features
- WCCP
- ASA CX SSP
- Many application inspection features (see Release Notes)
ACME Phase 4 – ASA Clustering

- ACME used clustering for a high speed data center where throughput and max connections were critical.
- With 8 ASA 5585-60s this cluster could achieve an approximate max throughput of 112GB with 56 million concurrent connections.
- Each ASA is dual homed via VPC to an upstream Nexus 7K.
Phase 4 Summary

- In order for ACME to scale their new high speed data center they required all firewalls in their infrastructure be active.
- This facilitated a migration from an Active Standby ASA failover model to ASA clustering.
- ACME opted to build the cluster in transparent (L2) mode using port channels for load-sharing and link redundancy.
- This architecture meets their requirement for highly available data center firewalls.
- None of the unsupported features with clustering were in play for this architecture.
- ACME also feels that clustering will enable them to split the firewalls across active data center in the future after feasibility testing.
ACME Phase 5
Application Visibility at the Edge
ACME Phase 5: Edge Application Visibility

- Like most companies, ACME leaves tcp/80 and tcp/443 unfiltered for outbound traffic, leading to concerns about what’s leaving the network.
- ACME security leadership decided to increase their visibility of all traffic types leaving the campus zone.
- Privately, ACME leadership is very concerned about confidential data leaking through well-known ports (e.g., HTTP/HTTPS).
- Application visibility will provide a more detailed means for applying security policy and also enforcing ACME’s new ethical workplace.
- ACME security team strongly desires to implement an identity-based security policy that includes content filtering (URL, application etc).
Application Visibility and Control Options

- Netflow is a good choice for gaining visibility into the network
- It will require a “collector” for collecting and parsing Netflow data
- Netflow is very useful when ports, protocols and payloads are known
- Network Based Application Recognition (NBAR) is another option in routers as a tool for monitoring application activity; unfortunately it has been limited in keeping up with new applications
- Cisco has a Web Security Appliance (WSA) that is a proxy server for analyzing application data over HTTP, FTP and HTTPS
- ASA firewalls have long had the ability to do application inspection but visibility into well known ports has been limited
ASA CX Deployment For Context Aware Firewall

- ACME recently deployed new firewalls in L2 mode
- VLAN based architecture scales easily for campus environment
- ACME has mapped user groups in AD for policy and requires identity based firewalling
- ASA CX (Context Aware) firewall blade is an option
What is ASA CX?

- ASA CX is firewall blade that goes into a 5585 chassis (SSP-10 or 20)
- It utilizes the ASA 5585 architecture for packet processing and then eligible flows are passed into the ASA CX blade via the backplane
- ASA CX is an application firewall which attempts to provide visibility and granular control over applications that use well known ports as well as applications that port hop
- Has a separate management plane from ASA and does not run ASA code
- Configured mostly via GUI with some troubleshooting tools via the CLI
- Allows ACME to provide very specific controls around common web applications such as Facebook, YouTube, LinkedIn, etc
ASA CX Blade is an Application Firewall

- ASA CX blade uses data plane of ASA 5585 chassis so if packets are dropped by firewall rule then CX blade will never have visibility
- Can be set to fail-open or fail-close
- Uses Modular Policy Framework (MPF) for redirecting all or specific flows to CX blade
ASA CX Granular Facebook Policy

Policy Name: Facebook Granular Controls

Enable policy: On
Policy Action: Allow

Source:
- Any
- Create new object

Destination:
- Any
- Create new object

Service:
- Any
- Create new object

Application:
- Facebook Notes
- Facebook General
- Facebook Places
- Create new object

Set application behaviors:
- Facebook General:
  - Install: Allow
  - Post: Deny
  - Tag: Deny

- Facebook Notes:
  - Post: Deny
  - Tag: Deny

- Facebook Places:
  - Post: Deny
  - Tag: Deny

Profile:
- File filtering action profile: Select one File filtering profile
- Web reputation action profile: Select one Web reputation profile

Create new object
Phase 5 Benefits and Challenges

- Many solutions to collect data and application visibility from network
- ASA CX is a blade for the 5585-10 and 5585-20 chassis
- ASA and ASA CX use two different code bases and are managed via two separate GUIs—ASDM and Cisco Prime Security Manager (PRSM)
- ASA CX provides visibility to more than 1000 applications using well-known ports
- Granular policies can be created to block/permit on application, URL category, user/group, and web reputation
- Placed at the internet edge for most efficient operation
- See BRKSEC-2020 for more information on ASA CX blade
Summary

ACME’s Five Phase Deployment
ACME’s Network Post Deployment

- ACME installed ASA SM blades into their legacy Catalyst 6500 switch chassis which was the first step towards an identity based security policy.
- ACME also deployed ASA firewalls in L2 mode using clustering for load sharing and maximizing the firewall architecture with all units active.
- Like many networks, ACME’s virtual host deployment far outpaced their physical server infrastructure. Virtual ASA helped push their security policy into the virtual layers.
- With the private cloud initiative, ACME became more granular in their security policy with regards to virtual machine attributes and the VSG allowed them to meet their security and compliance requirements.
- Finally, ASA CX gives them an option for granular application firewalling in the ASA family which supports ACME’s interest in a security policy that covers identity and content filtering.
Reference Links


Complete Your Online Session Evaluation

- Give us your feedback and you could win fabulous prizes. Winners announced daily.
- Receive 20 Passport points for each session evaluation you complete.
- Complete your session evaluation online now (open a browser through our wireless network to access our portal) or visit one of the Internet stations throughout the Convention Center.

Don’t forget to activate your Cisco Live Virtual account for access to all session material, communities, and on-demand and live activities throughout the year. Activate your account at the Cisco booth in the World of Solutions or visit www.ciscolive.com.
Recommended Reading

Cisco Firewalls by Alexandre Moraes

Cisco ASA, All-in-One Firewall (2nd edition) by Jazib Frahim and Omar Santos
Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions, booth 1042
- Come see demos of many key solutions and products in the main Cisco booth 2924
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
  - Facebook: https://www.facebook.com/ciscolineus
  - Twitter: https://twitter.com/#!/CiscoLive
  - LinkedIn Group: http://linkd.in/CiscoLI