CONTENTS

Introduction 4
  New in this Update 5
  Products and Releases 6
  Assumptions 7
Solution Overview 7
  Architecture 7
  Definitions 8
Design Considerations for Hosted Firewall and VPN Services 28
  NGFWv Sizing and Performance 33
  ASA v Sizing and Performance 34
  CSR1000v Sizing and Performance 34
  CSR1000v in SMB Designs 35
  NGFWv and ASA v in SMB Designs 36
  NGFWv, ASA v, and CSR1000v Licensing 36
  AnyConnect Licensing 36
Design Considerations for Hosted Web Security Services 37
  Web Security as a Service Tiers Example 37
  WS A v Sizing and Performance 38
  WS A v on UCS 39
  WS A v in SMB Designs 39
  WS A v Licensing 40
  WS A v Monitoring Profile and Reports 40
Design Considerations for Hosted Email Security Services 45
  Email Security as a Service Tiers Example 46
  ES A v Sizing and Performance 46
  ES A v on UCS 47
  ES A v in SMB Designs 47
  ES A v Licensing 47
  ES A v Monitoring Profile and Reports 47
Design Considerations for Advanced Malware Protection 51
  AMP Private Cloud Virtual Appliance 51
  AMP Threat Grid 54
Design Considerations for Distributed Denial of Service (DDoS) for the IaaS WAN Edge 55
Service Fulfillment Design Considerations 58
  UBIqube MSActivator Sizing Requirements 59
  Data Retention Requirements 59
  Service Provider Administrator Provision Requirements 60
Solution Validation 61
  Provisioning Workflow 61
  Creating the Service Tiers 62
  UBIqube MSActivator Common Operations 78
  Creating Delegation Profiles 79
  Creating Managers 83
  Creating Devices 86
SMB Design Guidance 94
Concluding Remarks 101
About the Authors 101
Appendix A—References 102
Appendix B—ESA High Availability Design Considerations 103
  Direct Server Return 103
  DNS Round Robin 105
  ESA Clustering 107
Appendix C—VMDC 2.3 Design Considerations 111
Appendix D—HSS Enterprise Designs Tested 113
  Enterprise Design 1b—ASAv, ESAv, WSAv, Public AMP, Public Threat Grid 113
  Enterprise Design 2—CSR1000v, ESAv, WSAv, Public AMP, Public Threat Grid 123
  Enterprise Design 3b—ASAv, CSR1000v, ESAv, WSAv, Public AMP, Public Threat Grid 134
  Enterprise Design 4—ASAv, ESAv, WSAv, Private AMP Shared and Private Threat Grid 151
  Enterprise Design 5—ASAv, ESAv, WSAv, Private AMP Dedicated and Private Threat Grid 152
Appendix E—HSS SMB Designs Tested 153
  SMB Design 1b—ASAv, Shared ESAv, Shared WSAv, Private AMP Shared and Private AMP Threat Grid 153
  SMB Design 2b—ASAv, Shared ESAv, Shared WSAv, Private AMP Dedicated and Private AMP Threat Grid 172
Cisco Hosted Security as a Service

Introduction

Increasingly, enterprise and small/medium business (SMB) customers are adopting cloud services from service providers more than in previous years. Cost savings, staffing shortages, and gaps in technology expertise are a few of the drivers that these businesses face. This trend is expected to accelerate over the next several years.

In response, service providers are introducing more cloud service offerings at a faster pace to meet this increase in demand. They provide their customers with a full suite of services that span collaboration, video, security, networking, and disaster recovery solutions.

The Cisco Hosted Security as a Service (HSS) solution enables service providers to deliver cost effective, managed security services to enterprise and SMB customers. These customers are challenged with maintaining a secure infrastructure and controlling costs, and often lack security expertise. By adopting Cisco HSS managed security services, service providers can help customers reduce their IT security costs, and provide up-to-date security protection while offloading security management operations.

This HSS Cisco Validated Design (CVD) includes the following Cisco virtual security appliances: Cisco Next Generation Firewall (NGFW), Cisco Adaptive Security Virtual Appliance (ASAv), Cisco Cloud Services Router (CSR1000v), Cisco Web Security Virtual Appliance (WSAv), Cisco Email Security Virtual Appliance (ESAvg), and Cisco Advanced Malware Protection Private Cloud Virtual Appliance (AMPv). These virtual appliances provide firewall, VPN, content security, and file reputation services. The HSS solution resides in the service provider data center and can be managed directly by the service provider, the Cisco Cloud and Managed Services (CMS) team, or by a third-party managed service provider.

Cisco has partnered with UBIqube for service provisioning, monitoring, security event management, and reporting of the HSS solution. UBIqube provides true multitenant security domain management with the capability to integrate with cloud orchestration and with Business Support Systems (BSS)/Operations Support Systems (OSS) solutions.

With the Cisco HSS solution, service providers benefit in the following ways:

- Mitigation of financial, technology, and market risks by using virtual machines instead of physical security appliances—Service providers avoid the risks associated with upfront investments in specific hardware and with future technology obsolescence.
• Acceleration of time to revenue by offering services that use virtual platforms in the cloud infrastructure foundation.

• Increased average revenue base—Bundling multiple service offerings to the same customer increases the spending of existing customers, and in turn will increase the number of enterprise customers through broadened service offerings.

• Proven technology solution—Built with industry-standard hardware and enterprise-class virtual security software (email, web, firewall, and so on).

• Reduced CapEx and OpEx in offering the service(s)—Because of a lower initial price as well as increased automation and standardization.

• Competitive differentiation—Ability to offer a variety of bundled services along with multiple service tiers and service-level agreements (SLAs).

The Cisco HSS design can be deployed on a variety of different Infrastructure as a Service (IaaS) solutions. HSS has been tested on Cisco service provider reference architectures. The service provider reference architectures are a family of designs known as the Cisco Virtualized Multiservice Data Center (VMDC). VMDC enables service providers to deliver bundles of cloud services including security, collaboration, IaaS, and application services. For more information about VMDC, see the following URL:

The most recent VMDC design is Cisco Virtual Services Architecture (VSA)1.0. VSA 1.0 uses virtual routers and firewalls to protect the tenant containers. For more information on VSA 1.0, see the VSA 1.0 Design Guide and Implementation Guide at the following URL:


The initial release of this guide was tested with the VMDC 2.3 architecture. VMDC 2.3 uses physical firewalls and routers to protect the tenant containers. For more information about VMDC 2.3, see the VMDC 2.3 Design Guide at the following URL:
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VMDC/2.3/design_guide/VMDC_2.3_DG.html*

In this update, we have extended virtualization support from VMware to also include KVM deployment options.

**New in this Update**

In this release, we added the following support to HSS:

• Cisco NGFWv

• Cisco Firepower Management Center

• UBIqube New SP and Customer Portal

• UBIqube Reporting with Kibana and Elastic Search

• New models: Cisco ASAv50 and Cisco WSA S600v

• Cisco ESAv on KVM

• Compute requirement expanded beyond UCS to include ANY x86 compute platform. Cisco UCS still recommended.
Products and Releases

The Cisco Hosted Security as a Service Solution uses the components listed in Table 1. Also shown are the HSS component requirement status and the tested release versions.

Table 1  
Cisco Hosted Security as a Service Solution Components

<table>
<thead>
<tr>
<th>Solution Component</th>
<th>Product</th>
<th>Release</th>
<th>Required/ Recommended/ Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSS</td>
<td>NGFWv</td>
<td>6.2.0.1</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>ASAv</td>
<td>9.6(2)</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>CSR1000v</td>
<td>3.16.5S</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>WSAv</td>
<td>10.1.1-235</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>ESAv</td>
<td>10.0.1-087</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>AnyConnect for Remote Access</td>
<td>4.2</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>AMPv</td>
<td>2.2.2</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>AMP Threat Grid 5500</td>
<td>2.1</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Firepower Management Center</td>
<td>6.2.0.1</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>UBIqube MSActivator Security</td>
<td>16.1.2</td>
<td>Recommended</td>
</tr>
<tr>
<td></td>
<td>Domain Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VMDC VSA</td>
<td>1.0</td>
<td>Recommended</td>
</tr>
</tbody>
</table>
Assumptions

Dependencies that are out of the scope of the Cisco HSS solution include the following:

- Service provider DNS
- Customer network DNS
- DomainKeys (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) security on DNS records for ESAv
- Public Key Infrastructure (PKI) and PKI Certificate Authority (CA)
- Out-of-band/offline update provisioning and management for WSAv and ESAv virtual machines

Solution Overview

Architecture

The Cisco HSS solution includes physical and virtual security appliances hosted in the service provider cloud to deliver managed security services for their business customers. Enterprise customers can also take advantage of this design guide by hosting security services for their own lines of business/divisions. The Cisco HSS solution offers multiple services to a single business customer such as email security, web security, firewall, next generation firewall with intrusion prevention, and VPN services. This CVD covers all of these services.
HSS includes solutions to address two different business customer segments: Enterprise and Small/Medium Business (SMB). The recommended solution depends on the number of users in the business. The threshold is currently recommended at 100 users. If the number of users is 100+, it is an enterprise design where the security appliances are dedicated to the customer. If the number of users is 5–100, it is an SMB design where the security appliances are shared with other customers.

The Cisco HSS solution uses three topology layers: the infrastructure layer, the services layer, and the orchestration layer, as shown in Figure 1 and Figure 2. HSS is the reference design for the Cloud and Managed Service Program (CMSP) Cloud and Managed Security service designation. If Cisco CMSP certifies the Cloud Managed Service implementation, the service can be sold as a Cisco Powered Service.

Definitions

**Customer** is a group of users representing a business. The business is offloading security services to the service provider.

**Tenant** is a collection of virtual machines in a container. In Enterprise designs the customer has a dedicated tenant container for its use. In SMB designs customers will use a shared tenant container with other customers.

*Figure 1* Hosted Security Solution Topology Layers—Enterprise Deployments

HSS Architecture – Enterprise (100 users+)

- **Orchestration Layer**
  - Delivered from service provider’s infrastructure
  - UBiqube MSActivator used as the Security Domain Manager
  - Orchestration SW interfaces with native appliance configuration mechanisms
  - All customer data lives inside the SP Cloud environment
  - Security on virtual form factor available today

- **Services Layer**
  - Service Layer
  - Policy, Analytics, Reporting

- **Tenant 1**
  - NGFWv
  - WSAv
  - ESAv
  - AMPv

- **Tenant 2**
  - CSR1000v
  - WSAv
  - ESAv
  - AMPv

- **Tenant 3**
  - ASAv
  - CSR1000v
  - WSAv+Shared AMP
  - ESAv+Shared AMP

- **Tenant 4**
  - NGFWv
  - CSR1000v
  - WSAv+Public AMP
  - ESAv+Public AMP

**Figure 2** Hosted Security Solution Topology Layers—SMB Deployments

- **Infrastructure**
  - VMware ESXi or KVM
  - Compute
  - Storage

- **Multi-Tenant Security Appliance**
  - Firepower 9300 or ASA5585

- **Threat Grid**

- **Policy**
  - Analytics
  - Reporting

- **SP existing orchestration, reporting & billing infrastructure**
  - Provisioning API
  - Reporting API
  - Billing API
## HSS Architecture – SMB (5-100 users)

### Orchestration Layer
- Policy
- Analytics
- Reporting

### Services Layer

<table>
<thead>
<tr>
<th>Customer 1</th>
<th>Customer 2</th>
<th>Customer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGFWv, ASAv, CSR1Kv</td>
<td>FWaaS/VPNaaS Policy</td>
<td>FWaaS/VPNaaS Policy</td>
</tr>
<tr>
<td>ESAv</td>
<td>ESaaS Policy</td>
<td>ESaaS Policy</td>
</tr>
<tr>
<td>WSAv</td>
<td>WSaaS Policy</td>
<td>WSaaS Policy</td>
</tr>
<tr>
<td>AMPv</td>
<td>File Reputation Policy</td>
<td>File Reputation Policy</td>
</tr>
</tbody>
</table>

### Infrastructure
- VMware ESXi or KVM
- Compute
- Storage
- Multi-Tenant Security Appliance: Firepower 9300 or ASA5585
- Threat Grid
Figure 3 shows the logical view of the connections available to the tenant container.

**HSS Architecture**

**OSS/BSS Integration**

**Orchestration**

**Security Services**

**Public IP Addresses**

**Public Internet**

**Public IP Addresses**

**Local LAN**

**HSS Designs**

The following container designs were tested in this updated design guide:

- Enterprise Design 1a—NGFWv, WSAv, ESAv with Public AMP and Public Threat Grid (see Figure 5)
- Enterprise Design 1b—ASAv, WSAv, ESAv with Public AMP and Public Threat Grid (see Figure 6)
- Enterprise Design 2—CSR1000v, WSAv, ESAv with Public AMP and Public Threat Grid (see Figure 7)
- Enterprise Design 3a—NGFWv, CSR1000v, WSAv, ESAv with Public AMP and Public Threat Grid (see Figure 8)
- Enterprise Design 3b—ASAv, CSR1000v, WSAv, ESAv with Public AMP and Public Threat Grid (see Figure 9)
- Enterprise Design 4a—NGFWv, WSAv, ESAv with Private AMPv Shared and Private Threat Grid (see Figure 10)
- Enterprise Design 4b—ASAv, WSAv, ESAv with Private AMPv Shared and Private Threat Grid (see Figure 11)
- Enterprise Design 5a—NGFWv, WSAv, ESAv with Private AMPv Dedicated and Private Threat Grid (see Figure 12)
• Enterprise Design 5b—ASAv, WSAv, ESAv with Private AMPv Dedicated and Private Threat Grid (see Figure 13)

• SMB Design 1a—NGFWv, Shared WSAv, Shared ESAv with Public AMPv and Public Threat Grid (see Figure 14)

• SMB Design 1b—ASAv, Shared WSAv, Shared ESAv with Public AMPv and Public Threat Grid (see Figure 15)

• SMB Design 1c—CSR1000v, Shared WSAv, Shared ESAv with Public AMPv and Public Threat Grid (see Figure 16)

• SMB Design 2a—NGFWv, Shared WSAv, Shared ESAv with Private AMPv Shared and Private Threat Grid (see Figure 17)

• SMB Design 2b—ASAv, Shared WSAv, Shared ESAv with Private AMPv Shared and Private Threat Grid (see Figure 18)

• SMB Design 2c—CSR1000v, Shared WSAv, Shared ESAv with Private AMPv Shared and Private Threat Grid (see Figure 19)

**HSS Design Selection**

Figure 4 should help guide you to the correct HSS design for the deployment scenario.

**Figure 4  HSS Container Design Selection Flow**

![HSS Container Design Selection Flow Diagram]

Are the # of users for the customer > 100?  
Yes  
No  
Consider SMB Design

Are Advanced Site to Site features needed?  
Yes  
No  
Consider Enterprise Design #3 NGFWv & CSR1000v or ASAv & CSR1000v

Are Advanced Remote Access features needed?  
Yes  
No  
Consider Enterprise Design #2 - CSR1000v

Are Advanced Routing features needed?  
Yes  
No  
Consider Enterprise Design #1 - NGFWv or ASAv

Enterprise Designs and SMB Designs can be delivered from the same virtualized data center
HSS Designs for Enterprise

The designs tested did not include all possible combinations that could be supported. For example, Enterprise Design #4 and Enterprise Design #5 were based off of Enterprise Design #1. The AMP combinations for Enterprise Design #1 were all tested. Table 2 shows the combinations that were tested as well as the combinations that are expected to work and are supported.

Table 2  Enterprise Design Table

<table>
<thead>
<tr>
<th>HSS Components</th>
<th>Public AMP and Public Threat Grid</th>
<th>Private AMPv Shared and Private Threat Grid</th>
<th>Private AMPv Dedicated and Private Threat Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGFWv, WSAv, ESAv</td>
<td>Enterprise Design #1a</td>
<td>Enterprise Design #4a</td>
<td>Enterprise Design #5a</td>
</tr>
<tr>
<td>ASAv, WSAv, ESAv</td>
<td>Enterprise Design #1b</td>
<td>Enterprise Design #4b</td>
<td>Enterprise Design #5b</td>
</tr>
<tr>
<td>CSR1000v, WSAv, ESAv</td>
<td>Enterprise Design #2</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>NGFWv, CSR1000v, WSAv, ESAv</td>
<td>Enterprise Design #3a</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>ASAv, CSR1000v, WSAv, ESAv</td>
<td>Enterprise Design #3b</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Figure 5  Design 1a—NGFWv, WSAv, ESAv with Public AMP and Public Threat Grid

HSS Enterprise Design #1a
NGFWv, WSAv, ESAv– Public AMP and Public Threat Grid

Note: Not showing redundant notes
Figure 6  Design 1b—ASAv, WSAv, ESAv with Public AMP and Public Threat Grid

HSS Enterprise Design #1b
ASAv, WSAv, ESAv– Public AMP and Public Threat Grid

Figure 7  Design 2—CSR1000v, WSAv, ESAv with Public AMP and Public Threat Grid

HSS Enterprise Design #2
CSR1000v, WSAv, ESAv– Public AMP and Public Threat Grid
The next two designs were based off of Enterprise Design #1. Enterprise Design #1, #4 and #5 are the
complete set of AMP deployment options. The complete set of Threat Grid options for Design #2 and 3 were not tested in this update, but are supported.

**Figure 10** Design 4a—NGFWv, WSAv, ESAv with Private AMP and Private Threat Grid

**HSS Enterprise Design #4a**
NGFWv, WSAv, ESAv – Private AMPv Shared and Private Threat Grid

![Diagram of HSS Enterprise Design #4a](image)

**Figure 11** Design 4b—ASAv, WSAv, ESAv with Private AMP and Private Threat Grid

**HSS Enterprise Design #4b**
ASAv, WSAv, ESAv – Private AMPv Shared and Private Threat Grid

![Diagram of HSS Enterprise Design #4b](image)
The Customer 1 site represents an enterprise site where directory and naming services run locally. The mail server could be hosted locally, hosted by the service provider in the Tenant 1 Container Private Zone, or hosted in the cloud (for example, Office365). The Customer 1 site is connected with a local
CPE, which uses either MPLS or IPSec VPN to connect to the service provider. The traffic terminates on the ASR9000. The ASR9000 inserts the traffic into the correct VLAN/VXLAN and delivers it to the Tenant 1 Expanded Gold Container, which is running on UCS B-Series virtualized data center. The tenant container is protected by the firewall services. The email and web security services run in the Tenant 1 DMZ Zone. Tenant 1 Private Zone hosts general purpose compute that can be used to host a wide variety of enterprise applications. SP Management applications should be deployed in a segmented LAN that is protected by a dedicated firewall. Access to and from the Internet flows through the Tenant 1 container with the ASAv and/or CSR1000v protecting the container with firewall services.

The design choice between enterprise designs depends on the requirements of the service. Table 3 shows the current recommendations for the expected requirements. Design selection for service is included in the HSS Service Creation program. Consult your Cisco account team if interested in this program.

**Table 3  Recommendations for HSS End Customer Enterprise Designs Expected Requirements**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Design 1—NGFWv or ASAv, WSAv, ESAv Public AMP</th>
<th>Design 2—CSR1000v, WSAv, ESAv Public AMP</th>
<th>Design 3—NGFWv or ASAv, CSR1000v, WSAv, ESAv Public AMP</th>
<th>Design 4—NGFWv or ASAv, WSAv, ESAv Private AMPv Shared</th>
<th>Design 5—NGFWv or ASAv, WSAv, ESAv Private AMPv Dedicated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-to-site VPN—Basic (IPSec VPN)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Site-to-site VPN—Advanced (DMVPN, Easy VPN, FlexVPN)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote access VPN—Basic (SSLVPN and IPSec/IKEv2 Cisco AnyConnect 4.1 or later)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Remote access VPN—Advanced (Clientless, WSA SSO)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Firewall—Basic (zone-based firewall)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Firewall—Advanced (URL Filtering, identity-based firewalling, device type-based enforcement)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AMP Threat Grid—(File reputation, analysis, and retrospection)</td>
<td>Public</td>
<td>Public</td>
<td>Public</td>
<td>Private</td>
<td>Private</td>
</tr>
<tr>
<td>Routing protocols—Basic (RIP, BGP, EIGRP, PBR)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Routing protocols—Advanced (GRE, VRF-Lite, Multicast, LISP)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced features—MPLS, Application Experience, OTV, VPLS, EoMPLS</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The CSR1000v and ASAv configurations for the enterprise designs are included in the Appendix.

**HSS Designs for SMB**

The SMB designs tested did not include all possible combinations that could be supported. Table 4 shows the combinations that were tested as well as the combinations that are expected to work and are supported.
The SMB Designs #1 and #2 tested in the update with the most likely AMP options. All combinations were not tested but are expected to be supported.

**Table 4**  
**SMB Design Table**

<table>
<thead>
<tr>
<th>HSS Components</th>
<th>Public AMP and Public Threat Grid</th>
<th>Private AMPv Shared and Private Threat Grid</th>
<th>Private AMPv Dedicated and Private Threat Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared NGFWv, Shared WSAv, Shared ESAv</td>
<td>SMB Design 1a</td>
<td>SMB Design 2a</td>
<td>Supported</td>
</tr>
<tr>
<td>Shared ASAv, Shared WSAv, Shared ESAv</td>
<td>SMB Design 1b</td>
<td>SMB Design 2b</td>
<td>Supported</td>
</tr>
<tr>
<td>Shared CSR1000v, Shared WSAv, Shared ESAv</td>
<td>SMB Design 1c</td>
<td>SMB Design 2c</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**Figure 14**  
**SMB Design 1a—NGFWv, Shared WSAv, Shared ESAv with Public AMP and Public Threat Grid**

**HSS SMB Design #1a**  
Shared NGFWv, Shared WSAv, Shared ESAv—Public AMP and Public Threat Grid
**Figure 15  ** SMB Design 1b—ASA, Shared WSv, Shared ESA with Public AMP and Public Threat Grid

**HSS SMB Design #1b**

Shared ASA, Shared WSv, Shared ESA– Public AMP and Public Threat Grid

![Diagram of SMB Design #1b](image)

**Figure 16  ** SMB Design 1c—CSR1000v, Shared WSv, Shared ESA with Public AMP and Public Threat Grid

**HSS SMB Design #1c**

Shared CSR1000v, Shared WSv, Shared ESA– Public AMP and Public Threat Grid

![Diagram of SMB Design #1c](image)
Figure 17  **SMB Design 2a—NGFWv, Shared WSAv, Shared ESAv with Private AMPv and Private Threat Grid**

HSS SMB Design #2a

Shared NGFWv, Shared WSAv, Shared ESAv– Private AMP Shared and Private Threat Grid

![Diagram: SMB Design 2a]

Figure 18  **SMB Design 2b—ASA, Shared WSAv, Shared ESAv with Private AMPv and Private Threat Grid**

HSS SMB Design #2b

Shared ASA, Shared WSAv, Shared ESAv– Private AMP Shared and Private Threat Grid

![Diagram: SMB Design 2b]
The Customer 1–3 sites each represent an SMB site where directory and naming services run locally. The mail server could be hosted locally or hosted in the cloud (for example, Office365). The Customer 1–3 sites are connected with a local CPE, which uses either MPLS or IPSec VPN to connect to the service provider. The traffic terminates on the ASR9000. The ASR9000 inserts the traffic into the correct VLAN/VXLAN and delivers it to the Shared Tenant Gold Container, which is running on UCS B-Series virtualized data center. The shared tenant container is protected by the firewall services. The email and web security services run in the Shared Tenant DMZ Zone. SP Management applications should be deployed in a segmented LAN that is protected by a dedicated firewall. Access to and from the Internet flows through the Shared Tenant container with the NGFWv, ASA and/or CSR1000v protecting the shared container with firewall services.

The ASA configurations for the SMB designs are included in the Appendix.

HSS has also been validated with the VMDC 2.3 release. The architecture is described in Figure 20. Refer to Appendix C—VMDC 2.3 Design Considerations, page 111 for further details.
Adding WSAv into the VSA 1.0 architecture results in the web traffic flow shown in Figure 21. All users at the tenant’s office will have the WSAv setup in their web clients, and all web traffic will be protected by the WSAv. The line in blue below initiated from Tenant 1 Site represents a user initiating a web request in their browser. The WSAv will process the request, and if it is allowed, will follow the yellow line to reach the Internet.

The WSAv can be deployed as an explicit web proxy, where the user has adjusted their network or browser settings to point directly to the WSAv. The WSAv can also be deployed to provide transparent redirection, where no customer endpoint changes are required. For Design 1, transparent redirection is provided by WCCP in the CSR1000v. For Design 2 and 3, transparent redirection is provided by the ASAv using Policy Based Routing (PBR).
Figure 21  Web Traffic Flow for Explicit Proxy

HSS Enterprise Deployment
ASA v Web traffic flow – Explicit Proxy

In Figure 22, the line in blue below initiated from Tenant 1 Site represents a user initiating a web request in their browser. The CSR1000v uses WCCP to redirect the web traffic to the WSAv transparently. The WSAv processes the request, and if it is allowed, follows the yellow line to reach the Internet.
In Figure 23, the line in blue below initiated from Tenant 1 Site represents a user initiating a web request in their browser. The ASAvs will use PBR to redirect the web traffic to the WSAv transparently. The WSAv will process the request, and if it is allowed, will follow the yellow line to reach the Internet.
Email flows can come from the customer-hosted email, from the service provider-hosted email, or cloud email (for example, Office365) as shown in Figure 24 and Figure 25. Inbound email flows in from the Internet following the blue line. The public DNS MX Record for the email server needs to point at the ESAv instead of the email server. The ESAv processes the email and delivers it to the email server following the yellow line if it is allowed to flow.

**Figure 24  Inbound Email Flow for Customer Hosted Email**

**HSS Enterprise Deployment**
Customer Hosted Email Inbound Flow

**Figure 25  Inbound Email Flow for Service Provider Hosted Email**

**HSS Enterprise Deployment**
Service Provider Hosted Email Inbound Flow
UBiqube MSActivator acts as the security domain manager in the Cisco HSS solution. The MSActivator framework abstracts the fulfillment of any vendor device to create a common service activation layer (see Figure 26).

**Figure 26**  
**UBiqube MSActivator Architecture**

**HSS Security Domain Manager – UBiqube MSActivator**

The MSActivator is engineered as a scalable telco grade, multitenant, and vendor-agnostic orchestration system. The framework simplifies device or element configuration and the activation and management of services. It features Open APIs to integrate with legacy OSS systems and SDKs for customization and integration of new vendors devices.

For more information on UBiqube, see the following URL: [http://www.ubiqubesolutions.com/](http://www.ubiqubesolutions.com/).

The Cisco HSS solution in this design guide supports VMware ESXi 5.5 or later. The following VMware features are supported by the security virtual appliances in this validated design:

- VM Templates (OVAs)
- VMware Clone
- VMware vMotion
- VMware Storage vMotion
- VMware High Availability (HA)
- VMware Site Recovery Manager (SRM)
- VMware Identity Feature
- Boot from SAN

In this update, in addition to VMware virtualization, we have confirmed the following components with KVM: NGFWv, ASAv, CSR1000v, ESAv, WSAv and UBiqube MSActivator.
Design Considerations for Hosted Firewall and VPN Services

HSS includes three options for hosted firewall and VPN services:

- **NGFWv—6.2.0.1**
- **ASAv—9.6(2) or later**
- **CSR1000v—3.16.5S or later**

The Cisco NGFWv, ASAv and CSR1000v are virtual appliances that provide firewall and VPN services. HSS uses these security services to create a virtual private cloud for each tenant.

The Cisco NGFWv is the virtual form of the physical Firepower Intrusion Prevention Service (IPS) appliance and the physical ASA. There are two management solutions for NGFWv: Firepower Management Center (FMC) and Firepower Device Manager (FDM). FMC comes in a physical or virtual form. It can manage up to 50 domains, so as a maximum we could share one FMC across 50 tenants. FMC was tested in this CVD update. FDM is the embedded device manager within the NGFWv image. FDM was tested in this update, it is a subset of what FMC can do. You must use either FMC or FDM, you cannot use both for a given NGFWv.

The Cisco ASAv is the virtual form of the physical Cisco ASA. The ASAv supports all the physical ASA features except multi-context and clustering. A physical ASA is also an option with multi-context mode. Refer to Appendix C—VMDC 2.3 Design Considerations for more information on this design.

The Cisco CSR1000v is the virtual form of a physical Cisco Aggregation Services Router (ASR), which runs IOS XE. The CSR1000v supports selected features in IOS XE based on targeted use cases including support for virtual private clouds.

Firewall as a Service includes two functional areas: standard firewall and advanced firewall features.

- **Standard features** include stateful inspection, application inspection, Network Address Translation (NAT), encrypted traffic inspection, and protocol inspection.
- **Advanced firewall features** include identity-aware policy enforcement, malware traffic detection and blocking, botnet traffic filter, voice, and video security.
Figure 27 shows an example of Firewall Security as a Service.

**Firewall as a Service: FWaaS**

- **Centralized Management and Reporting**
  - Firewall Support
    - Stateful inspection
    - Application inspection
    - Network address translation
    - Encrypted traffic inspection
    - Protocol inspection
  - Advanced Firewall
    - Identity-aware policy enforcement
    - Malware traffic detection and blocking
    - Botnet traffic filter
    - Voice and video security

**NGFWv, ASAv or CSR1000v**

**Per throughput and per feature service pricing**
Figure 28 shows an example of Firewall as a Service Tier.

**Figure 28  **Firewall as a Service Tier Example  

Firewall-aaS Tiers Example

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Service Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Bronze</td>
</tr>
<tr>
<td>Network Address Translation</td>
<td>NAT/PAT</td>
<td>✓</td>
</tr>
<tr>
<td>Stateful Inspection</td>
<td>L3 firewall</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Transparent firewall</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Proxy authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application hosting private zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application control (IM, peer to peer)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Voice security support</td>
<td></td>
</tr>
<tr>
<td>High Availability</td>
<td>Within SP data center</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Between SP data centers</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Customer self service portal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Streamlined management</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Auto generated reporting</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Custom reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data log retention (1 month)</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Extended data log retention (&gt;1 month)</td>
<td>✓</td>
</tr>
</tbody>
</table>

The VPN as a Service (see Figure 29 and Figure 30) includes two functional areas: remote access VPN and site-to-site VPN features.

**Figure 29  **VPN as a Service  

VPN as a Service: VPNaaS

Centralized Management and Reporting

VPN Services
- Remote access VPN
  - IPSec, SSL VPN
  - Session persistence (always on VPN)

VPN Services
- Site-to-site VPN through Internet FW

NGFWv, ASAv or CSR1000v

Per throughput per user service pricing
Remote Access VPN support is provided by the ASAv with the Cisco AnyConnect Mobility Client (currently at version 4.2). Cisco NGFWv Remote Access support will be available in 6.2.2. Though the VPN can be accessed in a Clientless mode, it is expected that this will be a less popular deployment model due to the increased cost of the license consumed for Clientless access. As enterprises move more toward consumerized employee devices, thereby wanting less corporate software footprint on them, Clientless VPN will become more popular.

The VPN service uses either the IPSec (IKEv2) or the SSL (TLS 1.2 or DTLS) protocol to configure the tunnel from the Client (AnyConnect) to the Head End (NGFWv or ASAv). The tunnel is established following a successful secure authentication handshake. This is where the Client agrees to trust the Head End Identity (through an X.509 certificate) and the Head End verifies the Client Identity by using one of the following methods:

- RADIUS
- RADIUS with password expiry (MSCHAPv2) to NT LAN Manager (NTLM)
- RADIUS one-time password (OTP) support (state and reply message attributes)
- RSA SecurID (including SoftID integration)
- Active Directory or Kerberos
- Embedded certificate authority (CA)
- Digital certificate or smartcard (including machine certificate support), auto- or user-selected
- Lightweight Directory Access Protocol (LDAP) with password expiry and aging
- Generic LDAP support
- Combined certificate and username or password multifactor authentication (double authentication)

When the tunnel is established, it is critical that the ASAv has NAT translation and firewall rules defined. This ensures that the VPN traffic coming to and from the clients can reach the customer tenant.
site and any private cloud services offered in the private zone and DMZ. Examples of an ASAv configured for a basic AnyConnect SSL VPN by using Basic Authentication are documented in Appendix D—HSS Enterprise Designs Tested, page 113.

The AnyConnect client comes with many popular optional features. These features can be enabled or disabled from the Head End through automatic provisioning. The same provisioning can push the client initially to supported endpoints (Windows 8 and 8.1, Windows 7 32-bit [x86] and 64-bit [x64], Mac OS X 10.8+ and Linux Intel [x64]) when they first establish a web connection with the Head End. Some of these features include:

- Optimal Gateway Selection
- Administrator controlled split-tunneling network access policy
- Cisco Hostscan—Posture checking of the client for AV/AS, FW, running processes and more.
- Always on VPN

For a list of all Cisco AnyConnect Mobility Client features, refer to the datasheet located at the following URL:

Site-to-site VPN feature support is provided by the Cisco NGFWv or ASAv. As an alternative to connecting tenant sites to the service provider using MPLS, a tenant site can also be connected using IPSec over the Internet.

The ASAv supports IPSec for site-to-site connections using either IKEv1 or IKEv2. The authentication methods supported for IKEv1 are Pre-shared Key and Device Certificate. For IKEv2, the supported authentication methods are Local Pre-shared Key, Local Device Certificate, Remote Peer Pre-shared Key, and Remote Peer Certificate Authentication.

It is recommended to use the Cisco Adaptive Security Device Manager (ASDM), which is a web-based manager that is bundled with the ASAv for configuring the initial site-to-site VPN tunnel. Once the initial ASAv CLI configuration is designed, you can deploy it as a template configuration in UBIqube MSActivator for each of the tenants.
### Figure 31  
Next Generation Firewall as a Service

**Next Gen Firewall as a Service: NG-FWaaS**

#### Centralized Management and Reporting

<table>
<thead>
<tr>
<th>Firewall Support</th>
<th>Next Gen Firewall</th>
<th>Next Gen IPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Stateful inspection</td>
<td>• Block allow traffic based on application criterias</td>
<td>• Network and transport layer protection policies</td>
</tr>
<tr>
<td>• Application inspection</td>
<td>• File control</td>
<td>• Predefined application intrusion policies</td>
</tr>
<tr>
<td>• Network address translation</td>
<td>• Reports based on discovery data, application blocked / allowed traffic</td>
<td>• Custom Intrusion Policies</td>
</tr>
<tr>
<td>• Encrypted traffic inspection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Protocol inspection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NGFWv / FMCv**

- Per throughput and per feature service pricing

### Figure 32  
Next Generation Firewall as a Service Tiers Example

#### NGFWaaS Tiers Example

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Service Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Visibility and Control (NGFW)</td>
<td>Network, User and Application Discovery</td>
<td>Bronze</td>
</tr>
<tr>
<td></td>
<td>Application Traffic filtering</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>URL Filtering</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>File Blocking (block xyz file type)</td>
<td>✔</td>
</tr>
<tr>
<td>Threat Protection (NGIPS)</td>
<td>IPS Basic Threat Protection Services (SNORT signatures)</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>IPS premium security signatures and content</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Security Intelligence Feeds</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>AMP (Advanced Malware Protection – disposition from the cloud/policy)</td>
<td>✔</td>
</tr>
<tr>
<td>High Availability</td>
<td>Configurable &quot;fail open&quot; – Appliance only</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>&quot;Fastpath&quot; and Trust Rules – Exclude/Include velocity</td>
<td>✔</td>
</tr>
<tr>
<td>Management</td>
<td>Streamline Management</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>IPS signature update</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Advanced/Custom Reporting</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Automated Policy Tuning – Advanced/Custom Policy Tuning</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Event Correlation – Customized Event Correlation Services</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Impact Analysis</td>
<td>✔</td>
</tr>
</tbody>
</table>

- Included
- Option
NGFWv Sizing and Performance

Table 5  NGFWv Disk, Memory, and Core Space per Tenant

<table>
<thead>
<tr>
<th>Model</th>
<th>Disk (GB)</th>
<th>Memory (GB)</th>
<th>vCPU</th>
<th>Maximum # vNICs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGFWv</td>
<td>50</td>
<td>8</td>
<td>4</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 6  NGFWv Performance and Sizing Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>NGFWv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput: FW + AVC</td>
<td>1.2 Gbps</td>
</tr>
<tr>
<td>Throughput: AVC + IPS</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Connections per second, with AVC</td>
<td>10,000</td>
</tr>
<tr>
<td>Concurrent sessions with AVC</td>
<td>100,000</td>
</tr>
<tr>
<td>VLANs maximum</td>
<td>50</td>
</tr>
<tr>
<td>Bridge groups maximum</td>
<td>25</td>
</tr>
</tbody>
</table>

ASA Sizing and Performance

The ASAv requires the disk, memory, and core space per tenant instance of the virtual machine that is shown in Table 7.

Table 7  ASAv Disk, Memory, and Core Space per Tenant

<table>
<thead>
<tr>
<th>Model</th>
<th>Disk (GB)</th>
<th>Memory (GB)</th>
<th>vCPU</th>
<th>Maximum # vNICs Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASAv5</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>ASAv10</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>ASAv30</td>
<td>16</td>
<td>8</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>ASAv50</td>
<td>16</td>
<td>16</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

Table 8  ASAv Performance and Sizing Metrics by Model

<table>
<thead>
<tr>
<th>Metric</th>
<th>ASAv5</th>
<th>ASAv10</th>
<th>ASAv30</th>
<th>ASAv50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful inspection throughput (maximum)</td>
<td>100 Mbps</td>
<td>1 Gbps</td>
<td>2 Gbps</td>
<td>10 Gbps</td>
</tr>
<tr>
<td>Stateful inspection throughput (multiprotocol)</td>
<td>50 Mbps</td>
<td>500 Mbps</td>
<td>1 Gbps</td>
<td>5 Gbps</td>
</tr>
<tr>
<td>AES VPN throughput</td>
<td>30 Mbps</td>
<td>125 Mbps</td>
<td>1 Gbps</td>
<td>3 Gbps</td>
</tr>
<tr>
<td>Connections per second</td>
<td>8,000 Mbps</td>
<td>20,000 Mbps</td>
<td>60,000 Mbps</td>
<td>120,000 Mbps</td>
</tr>
<tr>
<td>Concurrent sessions</td>
<td>50,000</td>
<td>100,000</td>
<td>500,000</td>
<td>2,000,000</td>
</tr>
<tr>
<td>VLANs</td>
<td>25</td>
<td>50</td>
<td>200</td>
<td>1024</td>
</tr>
<tr>
<td>Bridge groups</td>
<td>12</td>
<td>25</td>
<td>100</td>
<td>250</td>
</tr>
<tr>
<td>IPsec VPN peers</td>
<td>50</td>
<td>250</td>
<td>750</td>
<td>10,000</td>
</tr>
<tr>
<td>Cisco AnyConnect or Clientless VPN user sessions</td>
<td>50</td>
<td>250</td>
<td>750</td>
<td>10,000</td>
</tr>
</tbody>
</table>
Design Considerations for Hosted Firewall and VPN Services

**CSR1000v Sizing and Performance**

The CSR1000v requires the disk, memory, and core space per tenant instance of the virtual machine that is shown in Table 9.

**Table 9 CSR1000v Disk, Memory, and Core Space per Tenant**

<table>
<thead>
<tr>
<th>Throughput</th>
<th>SEC</th>
<th>AX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cores</td>
<td>Mem(GB)</td>
</tr>
<tr>
<td>10 Mbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>50 Mbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>250 Mbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>500 Mbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>2.5 Gbps</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>5 Gbps</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 10 lists key performance metrics for the CSR1000v deployment configurations for 16.3.1 ESXi/vSwitch.

**Table 10 CSR1000v Performance and Sizing Metrics ESXi/vSwitch**

<table>
<thead>
<tr>
<th>Metric</th>
<th>1vCPU</th>
<th>2vCPU</th>
<th>4vCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone based Firewall throughput</td>
<td>2.388 Gbps</td>
<td>2.799 Gbps</td>
<td>2.435 Gbps</td>
</tr>
<tr>
<td>NAT throughput</td>
<td>1.444 Gbps</td>
<td>2.084 Gbps</td>
<td>2.325 Gbps</td>
</tr>
<tr>
<td>IPSec AES VPN throughput</td>
<td>648 Mbps</td>
<td>715 Mbps</td>
<td>1.189 Gbps</td>
</tr>
<tr>
<td>IPSec 3DES throughput</td>
<td>122 Mbps</td>
<td>156 Mbps</td>
<td>231 Mbps</td>
</tr>
<tr>
<td>IPSec Concurrent sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SSLVPN throughput</td>
<td>200 Mbps</td>
<td>200 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>SSLVPN Concurrent sessions</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
</tbody>
</table>

Table 11 lists the key performance metrics for CSR1000v configurations for 16.3.1 KVM/vSwitch.

**Table 11 CSR1000v Performance and Sizing Metrics KVM/vSwitch**

<table>
<thead>
<tr>
<th>Metric</th>
<th>1 vCPU</th>
<th>2 vCPU</th>
<th>4 vCPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone based Firewall throughput</td>
<td>2.294 Gbps</td>
<td>2.654 Gbps</td>
<td>2.662 Gbps</td>
</tr>
</tbody>
</table>
CSR1000v in SMB Designs

SMB designs share a single CSR1000v instance across several tenants. The requirements of this design include the following:

- Overlapping tenant addressing is supported by using multi-VRF support in the CSR1000v.
- Remote access is supported for each tenant with SSLVPN. A unique group name is assigned to each tenant for mobile workers.

For more information, see the following URL:

NGFWv and ASAv in SMB Designs

SMB designs share a single NGFWv/ASAv instance across several tenants. The requirements of this design include the following:

- All tenants must have unique IP addressing and not overlap with other tenants. This may require NAT at the WAN edge.
- Each tenant is connected to the NGFWv/ASAv on a sub-interface. The number of sub-interfaces supported for the NGFWv is 50. The number of sub-interfaces supported by the four ASAv models ASAv5, ASAv10, ASASv30, and ASAv50 are 25, 50, 250, and 1024 respectively. This corresponds also to the number of VLANs supported in Table 6.
- For ASAv, remote access is supported for each tenant with SSLVPN. A unique group name is assigned to each tenant for mobile workers.

NGFWv, ASAv, and CSR1000v Licensing

NGFWv, ASAv, and CSR1000v use Cisco Smart Licensing. Features include the following:

- Simple purchase and activation
- Easy license management due to license pooling
- Automatic license activation upon provisioning
- Accurate and simple reporting of virtual security appliance usage in one portal

### Table 11  CSR1000v Performance and Sizing Metrics KVM/vSwitch

<table>
<thead>
<tr>
<th>Metric</th>
<th>1.686 Gbps</th>
<th>1.890 Gbps</th>
<th>1.531 Gbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT throughput</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPSec AES VPN throughput</td>
<td>620 Mbps</td>
<td>679 Mbps</td>
<td>857 Mbps</td>
</tr>
<tr>
<td>IPSec 3DES throughput</td>
<td>148 Mbps</td>
<td>148 Mbps</td>
<td>220 Mbps</td>
</tr>
<tr>
<td>IPSec Concurrent sessions</td>
<td>1000</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SSLVPN throughput</td>
<td>200 Mbps</td>
<td>200 Mbps</td>
<td>200 Mbps</td>
</tr>
<tr>
<td>SSLVPN Concurrent sessions</td>
<td>200</td>
<td>200</td>
<td>200</td>
</tr>
</tbody>
</table>

NGFWv, ASAv, and CSR1000v Licensing
AnyConnect Licensing

AnyConnect license management should be completed with a physical ASA. For details on how to order Cisco AnyConnect, refer to the following ordering guide:

Design Considerations for Hosted Web Security Services

The web security portion of Cisco HSS uses the virtual web security appliance, WSAv version 10.1.1-235. The solution includes two functional areas: web filtering and web security. Web filtering includes web usage controls, URL filtering, application visibility, and bi-directional control. Web security includes anti-malware protection and web content analysis. (See Figure 33.)

Figure 33  Web Security as a Service

Web Security as a Service: WSaaS

Centralized Management and Reporting

Web Filtering
- Web usage controls
- Application visibility
- Bi-Directional control
- Advanced Malware Protection

Web Security
- Anti-Malware protection
- Web content analysis

WSAv

Per user pricing model driven by features
Web Security as a Service Tiers Example

The tested and validated design includes three example service tiers that a service provider can offer their enterprise customers (see Figure 34).

Figure 34  Web Security as a Service Tiers Example

WSaaS Tiers Example

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Time Threat Protection Services</td>
<td>Web reputation filtering</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Malware scanning</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Acceptable Use Services</td>
<td>Web URL monitoring by category</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Web URL filtering (blocking)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Web application monitoring</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Web application control</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>SaaS access control</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Transparent user authentication</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Advanced Malware Protection</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Policy Control</td>
<td>Granular access and control policies</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>High Availability</td>
<td>Remote access and control policies</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Management</td>
<td>Included</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

WSAv Sizing and Performance

The WSAv requires the disk, memory, and core space per tenant instance of the virtual machine that is shown in Table 12.

Table 12  Disk, Memory, and Core Space per Tenant

<table>
<thead>
<tr>
<th>Model</th>
<th>Disk</th>
<th>Memory (GB)</th>
<th>Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>S000V</td>
<td>250 GB</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>S100V</td>
<td>250 GB</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>S300V</td>
<td>1024 GB</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>S600V</td>
<td>2.4 TB</td>
<td>24</td>
<td>12</td>
</tr>
</tbody>
</table>

The performance of a single instance of the WSAv, version 10.1 is shown in Table 13, where RPS is HTTP requests per second.

Table 13  WSAv 10.1 RPS Performance

<table>
<thead>
<tr>
<th>Performance Test Bundles</th>
<th>S600V</th>
<th>S300V</th>
<th>S100V</th>
<th>S000V</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sustained RPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note the following:
- All test runs are with Medium Policy Complexity and 25% SSL
- Sustained RPS to be used for sizing
- AMP Cloud: Files sent for analysis to the cloud. AMP Threat Grid: Files sent for analysis to the on-prem Threat Grid appliance

### WSAv on UCS

Sizing WSAv on Cisco Unified Computing System (UCS) should be performed with Cisco Content Security Product team experts.

### WSAv in SMB Designs

In this update, SMB designs are introduced that share a single WSAv across several tenants. The requirements of this design include the following:
- All tenants must have unique IP addressing and not overlap with other tenants. This may require NAT at the WAN edge. However, if the CSR1000v is deployed, you can use multi-VRF mode, which segments the tenant traffic.
- WSAv policy (recommended to be configured in this order):
  - Authentication realms must be created for every tenant so that the users can be authenticated against the tenant DNS and the user details can be captured in reporting.
Design Considerations for Hosted Web Security Services

- Identification profiles must be created for every tenant to describe the source IP addressing of the tenant traffic. The identification profile includes the authentication realm for the tenant.
- Access policies must be created for each tenant. The access policy includes the identification profile for the tenant.

WSAv Licensing

The HSS web security services used the WSAv Premium License in HSS solution testing. Providing anti-malware and anti-virus protection is the foundation for this service. URL filtering and application control are service options. If the end customer requires only web filtering and no malware protection, they would deploy the Web Security Essentials license.

WSAv Monitoring Profile and Reports

The set of WSAv SNMP objects that were tested in this CVD are defined in the WSAv Monitoring Profile shown in Figure 35 and Figure 36. Custom graphs and objects tracked are supported. The WSAv Monitoring Profile is an example of the data that can be monitored. Monitoring Profiles can be tailored to service provider specific requests.

Figure 35  WSAv Monitoring Profile—SNMP Polling
Table 14 lists the WSAv MIB objects used by the WSAv Monitoring Profile.

**Table 14  WSAv MIB Objects**

<table>
<thead>
<tr>
<th>WSAv MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacheBandwidthTotal1dayMean</td>
<td>Average bandwidth total in the last day (in Kb/sec)</td>
</tr>
<tr>
<td>cacheBandwidthTotal1hrMean</td>
<td>Average bandwidth total in the last hour (in Kb/sec)</td>
</tr>
<tr>
<td>cacheBandwidthTotal1weekMean</td>
<td>Average bandwidth total in the last week (in Kb/sec)</td>
</tr>
<tr>
<td>cacheBusyCPUPct</td>
<td>Percentage of busy time of CPU</td>
</tr>
<tr>
<td>cacheBandwidthSaving1hrMean</td>
<td>Average bandwidth savings in the last hour (in Kb/sec)</td>
</tr>
</tbody>
</table>
The full set of WSAv SNMP objects possible to monitor for 10.x is the same as 8.0 AsyncOS Web MIB; see the following URL: http://www.cisco.com/web/ironport/tools/web/8.0/asyncosweb-mib.txt

The service provider administrator can capture the WSAv access logs through the VM syslog to generate reports. Ubiquube has created a template file that when applied to the device creates a custom W3C log file format that is loaded into the WSAv. The log fields are shown in Table 15.

### Table 14 WSAv MIB Objects (continued)

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacheBwidthSaving1dayMean</td>
<td>Average bandwidth savings in the last day (in Kb/sec)</td>
</tr>
<tr>
<td>cacheBwidthSaving1weekMean</td>
<td>Average bandwidth savings in the last week (in Kb/sec)</td>
</tr>
<tr>
<td>cacheMaxResSize</td>
<td>Maximum resident size in KB</td>
</tr>
<tr>
<td>cacheTotalRespTime1hrMean</td>
<td>Average cache total response time in the last hour</td>
</tr>
<tr>
<td>cacheTotalRespTime1dayMean</td>
<td>Average cache total response time in the last day</td>
</tr>
<tr>
<td>cacheTotalRespTime1weekMean</td>
<td>Average cache total response time in the last week</td>
</tr>
<tr>
<td>cacheServerInKb</td>
<td>The number of KBs received by the proxy from remote servers.</td>
</tr>
<tr>
<td>cacheServerErrors</td>
<td>The number of HTTP errors while fetching objects.</td>
</tr>
</tbody>
</table>

### Table 15 Log Fields

<table>
<thead>
<tr>
<th>Log Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c-ip</td>
<td>Client IP address</td>
</tr>
<tr>
<td>cs-username</td>
<td>Client-to-server username</td>
</tr>
<tr>
<td>s-ip</td>
<td>Server IP address</td>
</tr>
<tr>
<td>cs(Referer)</td>
<td>Referer</td>
</tr>
<tr>
<td>cs-url</td>
<td>The entire URL</td>
</tr>
<tr>
<td>s-hostname</td>
<td>Data source or server IP address</td>
</tr>
<tr>
<td>s-port</td>
<td>Destination port number</td>
</tr>
<tr>
<td>sc-http-status</td>
<td>HTTP response code</td>
</tr>
<tr>
<td>sc-bytes</td>
<td>Response size (header + body)</td>
</tr>
<tr>
<td>Bytes</td>
<td>Max syslog message length</td>
</tr>
<tr>
<td>x-elapsed-time</td>
<td>Elapsed time</td>
</tr>
<tr>
<td>s-hierarchy</td>
<td>Hierarchy retrieval</td>
</tr>
<tr>
<td>cs(User-Agent)</td>
<td>User agent. This field is written with double-quotes in the access logs.</td>
</tr>
<tr>
<td>cs-uri</td>
<td>Request URI</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Timestamp in UNIX epoch</td>
</tr>
<tr>
<td>x-webcat-code-abbr</td>
<td>The URL category verdict determined during request-side scanning, abbreviated.</td>
</tr>
<tr>
<td>x-webcat-code-full</td>
<td>The URL category verdict determined during request-side scanning, full name.</td>
</tr>
<tr>
<td>x-mcafee-virus-name</td>
<td>McAfee specific identifier: (virus name). Field written with double-quotes in the access logs.</td>
</tr>
</tbody>
</table>
Table 15  Log Fields (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-mcafee-scanverdict</td>
<td>Request side DVS scan verdict</td>
</tr>
<tr>
<td>x-webroot-threat-name</td>
<td>Webroot specific identifier (threat name). This field is written</td>
</tr>
<tr>
<td></td>
<td>with double-quotes in the access logs.</td>
</tr>
<tr>
<td>x-webroot-scanverdict</td>
<td>Malware scanning verdict from Webroot</td>
</tr>
<tr>
<td>sc-result-code</td>
<td>Result code. For example: TCP_MISS, TCP_HIT</td>
</tr>
</tbody>
</table>

UBIqube WSAv default report requires these fields to generate the UBIqube reports.

---

Note

The full set of W3C logs can be found at the following URL:

For a WSA Dashboard Report example, please refer to Figure 37.

**Figure 37  WSA Dashboard Report**

The service provider administrator might be interested in the following reporting tabs on the WSAv:
- Reporting > System Capacity
- Reporting > System Status

The remainder of the reporting capabilities on the WSAv are mostly relevant to the end customer administrator. For some customers, monitoring the reports will be sufficient. If customers want guest or read-only access to the WSAv GUI, this is supported by UBIqube role-based access capabilities.

WSAv role-based access controls must also be used to ensure that the end customer does not upgrade
Design Considerations for Hosted Email Security Services

The email security portion of HSS uses the virtual email security appliance, ESAv, using AsyncOS 10.0.1-087 for email. (See Figure 38.)

The solution includes inbound email protection for the following:

- Spam defense
- Virus and malware defense
- SenderBase reputation scoring from Talos
- Content and outbreak filters

The ESAv Hypervisor support is limited to VMware ESXi only.
Email Security as a Service Tiers Example

The design includes only inbound email security. Figure 39 lists the three tested and validated service tiers that a service provider can offer their enterprise customers.

**Figure 39 Email Security as a Service Tier Example**

<table>
<thead>
<tr>
<th>Category</th>
<th>Feature</th>
<th>Service Tiers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Email Protection</td>
<td>Reputation scoring and SMTP blocking</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Anti-spam</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Outbreak filters, Sophos anti-virus</td>
<td>✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Inbound email content filtering</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Quarantine</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Advanced Malware Protection</td>
<td>✓</td>
</tr>
<tr>
<td>Outbound Email Protection</td>
<td>Anti-virus</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Outbound email content filtering</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Integrated RSA data loss prevention</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>DLP RSA enterprise manager integration (enterprise provided)</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Large volume</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Quarantine</td>
<td>***</td>
</tr>
<tr>
<td>Policy Control</td>
<td>Granular policy control</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Roaming users protection</td>
<td>***</td>
</tr>
<tr>
<td>High Availability</td>
<td>Within SP data center</td>
<td>✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Between SP data centers</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>Management</td>
<td>Self service portal</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Streamlined management</td>
<td>✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Auto-generated reporting</td>
<td>✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Custom reporting option</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Data log retention (1 month)</td>
<td>✓ ✓</td>
</tr>
<tr>
<td></td>
<td>Extended data log retention (&gt;1 month)</td>
<td>***</td>
</tr>
</tbody>
</table>

**ESAv Sizing and Performance**

The ESAv requires the disk, memory, and core space per tenant listed in Table 16.

**Table 16 Disk, Memory, and Core Space**

<table>
<thead>
<tr>
<th>Email Users</th>
<th>Model</th>
<th>Disk (GB)</th>
<th>Memory (GB)</th>
<th>Cores</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;1000</td>
<td>C100V</td>
<td>200</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>1000-5000</td>
<td>C300V</td>
<td>500</td>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>&gt;5000</td>
<td>C600V</td>
<td>500</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 17 lists the ESA message-per-second performance.

**Table 17 ESAv Performance—Message per Second**

<table>
<thead>
<tr>
<th>Test ID</th>
<th>Scanning Options &amp; Features</th>
<th>C100v</th>
<th>C300v</th>
<th>C600v</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIE000800000000000019</td>
<td>ipas+sbrs+sbnp+jumbo_mbox</td>
<td>3.21</td>
<td>6.69</td>
<td>11.4</td>
</tr>
<tr>
<td>SIE00080000000000001F</td>
<td>ipas+sophos+vf+sbrs+sbnp+jumbo_mbox</td>
<td>2.96</td>
<td>6.08</td>
<td>10.4</td>
</tr>
</tbody>
</table>
ESAv on UCS

Sizing ESAv on Cisco UCS should be done with Cisco Content Security Product team experts. The performance information in the previous section represents a specific deployment scenario. It is best to identify the correct performance test metric that matches the expected deployment scenario. Once you determine message per second, then accurate sizing can be done.

ESAv in SMB Designs

In this update, SMB designs are introduced that share a single ESAv across several tenants. The requirements of this design include the following:

- All tenants must have unique IP addressing and not overlap with other tenants. This may require NAT at the WAN edge. However, if the CSR1000v is deployed you can use multi-VRF mode, which segments the tenant traffic.
- ESAv policy (recommended to be configured in this order):
  - Each tenant should have content filters defined.
  - Each tenant should have a unique incoming mail policy defined that includes any content filters defined for the tenant.
  - No quarantine support per customer. If required, a dedicated ESAv is needed for the customer.

ESAv Licensing

HSS email security uses the Email Security Inbound License. Cisco did not validate the outbound email security; however, if a service provider wants to offer outbound email security services, the Email Security ESA-ESO-LIC= License will be required.

ESAv Monitoring Profile and Reports

The set of ESAv SNMP objects that were tested in this CVD are defined in the ESAv Monitoring Profile (see Figure 40). Custom graphs and objects tracked are supported. The ESAv Monitoring Profile is an example of the data that can be monitored. Monitoring Profiles can be tailored to service provider specific requests.
Figure 40   ESAv Monitoring Profile—SNMP Polling
ESA MIB objects that the ESAv Monitoring profile uses are as follows:

- ESAv MIB Object
- perCentCPUUtilization
- perCentMemoryUtilization
- perCentQueueUtilization
- workQueueMessages
- mailTransferThreads

**Note**

For the full set of ESAv SNMP objects available, see the following URLs:

http://www.cisco.com/web/ironport/tools/email/ASYNCOS-MAIL-MIB.txt

http://www.cisco.com/web/ironport/tools/email/IRONPORT-SMI.txt
The ESA reports are based off the default log subscription mail_logs. For an ESA Daily Report example, please refer to Figure 42.

Figure 42  ESA Daily Report Example

The service provider administrator can capture the mail logs through ESAv syslog to generate reports. UBIqube uses the standard format for the ESAv mail logs.

The service provider administrator might be interested in several reporting tabs on the ESAv:
- Reporting -> System Capacity
- Reporting -> System Status

The remainder of the reporting capabilities on the ESAv are mostly relevant to the end customer administrator. For some customers, monitoring the daily and monthly reports directly from the ESAv will be sufficient If customers want guest or read-only access to the ESAv GUI, this is supported by UBIqube role-based access capabilities.

ESAv role-based access controls must also be used to ensure that the end customer does not upgrade their level of service without service provider knowledge. The service provider must create a new role
Design Considerations for Advanced Malware Protection

In this design guide update, we have extended the email and web security support to also include Cisco Advanced Malware Protection (AMP).

Adding Cisco AMP provides the following benefits:

- Analyze emails and web traffic for threats, such as zero-day exploits hidden in malicious attachments or downloads
- Shorten the time to detection with retrospective alerts
- Track unknown files that have crossed the email or web gateway, with continuous analysis
- Uncover stealthy malware and understand how it works with advanced sandboxing
- Strengthen network defenses with proven threat intelligence from Talos

AMP Private Cloud Virtual Appliance

AMP Virtual Private Cloud Appliance (ASAv) is an on-premises, air-gapped private cloud deployment of Cisco AMP for Networks or Cisco AMP for Endpoints. The Cisco AMP Private Cloud Virtual Appliance delivers comprehensive advanced malware protection using big data analytics, policies, detections, and protections stored locally on premises. When the solution discovers an unknown suspicious file, it interacts with our intelligence database, the Cisco AMP threat intelligence public cloud, for file disposition lookup. Privacy policies and heavy regulations can limit the use of public clouds. The AMP Virtual Private Cloud Appliance gives organizations in industries, markets, or regions with strict privacy mandates an effective, highly secure alternative to the public cloud.

The Cisco AMP Virtual Private Cloud Appliance supports two deployment modes: “cloud proxy mode” and “air gap mode”.

In the cloud-proxy mode:

- An Internet connection is needed to complete disposition lookups
- All traffic from endpoint connectors is to the private cloud, but disposition lookup is subsequently performed between the private cloud and the AMP public cloud
- The SHA-256 hash of the file being inspected is the only data sent to the public AMP cloud from the AMP Virtual Private Cloud Appliance
- Content and software updates can be retrieved automatically from the AMP cloud directly to the AMP Virtual Private Cloud Appliance

In the air gap mode:

- No internet connection is needed to complete disposition lookups
- All traffic is between the connectors and the appliance only

with the correct entitlements for the end customer administrator.

The retention policy for log files is one year by default. It is configured globally for the UBIqube MSActivator. All customers will have same retention policy. All logs are easily visible from UBIqube MSActivator for one month. They are archived after a month. Access to the UBIqube MSActivator CLI is needed to retrieve the log files from the archive.

For guidance on High Availability support for ESA deployments, refer to Appendix B—ESA High Availability Design Considerations, page 103.
Disposition queries are handled by the private device. 

Figure 43 and Figure 44 illustrate how each deployment mode operates.

**Figure 43 Cloud Proxy Mode**
For HSS, the testing focused on using AMP for Networks, but we did confirm that AMP for Endpoints worked as expected for the dedicated Enterprise designs. AMP for Endpoints must be deployed as a dedicated AMPv for the customer because AMPv is not multi-tenant. SMB designs support AMP for Networks only.

AMPv was tested as a shared service for all tenants of the service provider. A dedicated AMPv for each tenant was also tested. The AMPv Hypervisor support is limited to VMware ESXi only.

The AMPv installation instructions can be found here:

We confirmed v2.2.2 but the most recent version of AMPv can always be found here:
http://sourcefire-apps.s3.amazonaws.com/fireAMP/PrivateCloud/PrivateCloud-Latest.ova

Table 18 shows various AMPv mode requirements.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Disk</th>
<th>Memory (GB)</th>
<th>vCPUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud mode</td>
<td>238 GB</td>
<td>32</td>
<td>8</td>
</tr>
<tr>
<td>Air gap</td>
<td>1 TB</td>
<td>128</td>
<td>8</td>
</tr>
</tbody>
</table>
WSAv and ESAv support AMPv in AsyncOS 10.0.
For more information, see the following URLs:

- http://www.cisco.com/go/amp

**AMP Threat Grid**

In this design guide update, we have extended the email and web security support to also include Cisco AMP Threat Grid. Cisco AMP Threat Grid is an advanced sandboxing technology that does file analysis for unknown files.

Adding Cisco AMP Threat Grid provides the following benefits:

- Accurately identifies attacks in near real time with context-focused security analytics
- Defends against threats from anywhere with the scale and power of a cloud service that analyzes millions of threats daily
- Accelerates threat detection and incident response capabilities with an easy-to-use REST API
- Improves existing security investments with pre-packaged and custom threat intelligence feeds
- Integrates with existing third-party security technologies, and takes advantage of AMP Threat Grid’s integration across the Cisco security portfolio


Table 19 provides AMP Threat Grid model and licensing details.

<table>
<thead>
<tr>
<th>Model</th>
<th>Maximum number of files analyzed per day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco AMP Threat Grid 5000</td>
<td>1500</td>
</tr>
<tr>
<td>Cisco AMP Threat Grid 5500</td>
<td>5000</td>
</tr>
</tbody>
</table>
Design Considerations for Distributed Denial of Service (DDoS) for the IaaS WAN Edge

In this design guide update, we have extended the reference IaaS architecture used for HSS. The ASR9000 is in the reference architecture to protect the WAN Edge. Cisco has partnered with Arbor Networks to deliver the ASR9000 vDDoS Protection solution. vDDoS runs on the Virtualized Services Module (VSM) in the ASR9000. The vDDoS solution with Arbor adds this to the architecture without consuming additional rackspace. Refer to Figure 45 for more information.

Figure 45  Cisco ASR9000 vDDoS Protection

Cisco ASR 9000 vDDoS Protection

Arbor Networks Threat Management System (TMS)  ASR 9000 with Virtual Services Module (VSM)  Cisco ASR 9000 vDDoS Protection “Powered By Arbor Networks”

Architectural Superiority  United Management  Scalable Performance  Reduced OPEX  Flexible Deployment
Figure 46 is a DDoS attacks overview. It shows the different types of DDoS attacks: Volumetric, TCP State-Exhausting Attacks, and Application layer for a common SP deployment scenario.

**DDoS attacks overview**

**TCP State-Exhausting Attacks**
- Targets *stateful* devices (load balancers, firewalls, application servers)
- Usually 1-10Gbps, but a lot of Mpps

**Volumetric Attacks**
- Overloads links
- 10-500 Gbps

**Application Layer Attacks**
- *Stealth* attacks, < 1Gbps, 100+ requests per sec
- No impact on infrastructure
- Huge load on applications

---

*Figure 46  DDoS Attacks Overview*
In Figure 47, the components of the vDDoS solution are highlighted where they will likely be deployed with HSS. The ASR9000 with vDDoS will do DDoS mitigation, and the Arbor TMS application will be hosted in the SP management zone and it will do DDoS detection.

The vDDoS solution as deployed in HSS above is focused on mitigating volumetric based attacks. This support has not been tested as part of this update, but has been tested by the ASR9000 team.

Please refer to the ASR9000 vDDoS Protection Data Sheet for more information:

- [http://arbornetworks.com/asr9000](http://arbornetworks.com/asr9000)
Service Fulfillment Design Considerations

For the HSS solution, Cisco partners with UBIqube for service fulfillment that includes the following:

- Service provisioning and activation
- License management
- Change management
- Service monitoring
- Updates
- Reporting

In this solution, Cisco used UBIqube MSActivator version 16.1.2 as a Security Domain Manager. UBIqube MSActivator abstracts the fulfillment of Cisco (and other vendor) devices to create a common service activation layer. It is a telco grade, multi-tenant, and vendor-agnostic orchestration system that simplifies element configuration, activation, and management of services.

The MSActivator is a converged, managed-services delivery platform structured around an Information Technology Infrastructure Library (ITIL)-based configuration management database. The MSActivator modules are operated through the unified web portal. The Virtual Security Operation Center (VSOC) allows for centralized provisioning, management, and monitoring of the devices and services. (See Figure 48.)

![UBIQUBE MSActivator](Figure 48)

HSS Security Domain Manager – UBIqube MSActivator

<table>
<thead>
<tr>
<th>Service Profiles</th>
<th>Web Portal GUI</th>
<th>3rd Party OSS/BSS</th>
<th>Verbs and Web Services API, Order Stack Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Designer</td>
<td>Templates and Objects</td>
<td>Web Services</td>
<td></td>
</tr>
<tr>
<td>OBMF Mediation Layer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Adaptor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Conf</td>
<td>Restore Conf</td>
<td>Update Firmware</td>
<td></td>
</tr>
<tr>
<td>Get Asset</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Adaptor (SDK)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Conf</td>
<td>Restore Conf</td>
<td>Update Firmware</td>
<td></td>
</tr>
<tr>
<td>Get Asset</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Southbound Interface</td>
<td>TELNET SSH HTTP</td>
<td>SNMP Syslog FTP Netflow</td>
<td>Openflow TR069</td>
</tr>
<tr>
<td>VOIP</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

340393
UBIQUBE MSActivator Sizing Requirements

The hardware size is determined by the number of managed devices, and the monitoring level of those devices.

- MSActivator offers various levels of monitoring:
  - Silver Monitoring checks the status of the devices and also polls the device with SNMP to build graphs according to key performance indicators (KPI).
  - Gold Monitoring collects device events to measure activity. Events are classified to reflect activity on a per-type basis.
  - Email Alert guarantees real-time event alerts for events that are occurring on devices (requires Gold Monitoring.).

It is best to use the new MSA sizing tool to determine exact hardware requirements for the deployment. UBIqube will provide access to the MSA sizing tool.

Data Retention Requirements

Service providers need to estimate how much disk space is needed for the deployment of all tenants. The estimate is largely based on the services that are deployed and the number of users. The guidance shown in Figure 49 is the method that we recommend for determining disk space requirements for archiving monitoring logs and reports.

Figure 49  Disk Space Requirements

<table>
<thead>
<tr>
<th>For WSA: 500 bytes per log</th>
<th>For ESA: Log entries are &gt; 500 bytes, the rule to follow</th>
</tr>
</thead>
<tbody>
<tr>
<td>- We have 0.1 http request per second / user, 8 hours a day which makes 2880 requests / user per day</td>
<td>- 350,000 accepted messages = 1GB</td>
</tr>
<tr>
<td>- With 500 bytes per log gives us 1.44 MB / user / day</td>
<td>- 2.8 million rejected messages = 1GB</td>
</tr>
<tr>
<td>- With 6 days / week, we have 8.64 MB / user / week</td>
<td>- We take also as a rule that for 1 accepted message we have between 5 and 10 rejected message so to be safe we will assume 10</td>
</tr>
<tr>
<td></td>
<td>- We have 20 mails / user / day, we will have: 200 KB / user / day</td>
</tr>
<tr>
<td></td>
<td>- With 6 days / week, we have 1.2 MB / user / week</td>
</tr>
</tbody>
</table>
**Service Fulfillment Design Considerations**

**Figure 50 and Figure 51** show sample outputs for the WSA and ESA from the MSA sizing tool.

### Figure 50  MSA Sizing Tool—WSA Sample Output

![Image of MSA Sizing Tool—WSA Sample Output]

### Figure 51  MSA Sizing Tool—ESA Sample Output

![Image of MSA Sizing Tool—ESA Sample Output]
Service Provider Administrator Provision Requirements

Service provider administrators need to deploy security services that support automation for provisioning, reporting, and billing. UBIqube MSActivator Security Domain Manager can integrate into a service provider’s cloud orchestration solution, if one exists.

There are two primary levels of service provider administrators: SP Service Administrator and SP Operations Activation Administrator.

UBIqube MSActivator Security Domain Manager enables the SP Service Administrator to do the following:

- Create the service tiers for each security service
- Integrate service into a billing system
- Define the data retention policy services
- Define the end customer level of access policy
- Define service provider operation level access policy

See the UBIqube MSActivator documentation for additional information.

UBIqube MSActivator Security Domain Manager enables the SP Operations Service Activation Administrator to do the following:

- Create a new customer
- Create/add service for the customer
- Provide customizable levels of access policy
- Monitor service and provide customizable reports to the end customer
- Assign data retention policy for the customer
- Manage user license

See the UBIqube MSActivator documentation for additional information.
Solution Validation

This section details the configuration of the HSS components and provisioning by using UBIqube MSActivator.

Figure 52 shows a sample HSS device configuration for service provider A (SPA). SPA-Admin is logged in to UBIqube MSActivator. The window shows three tenants: Customer 1 has one NGFWv, one ESAv, and one WSAv configured. Customer 2 has one ASAv, one ESAv, and one WSAv configured. Shared Tenant 1 has one CSR1000v, one ESAv, and one WSAv configured. SMB1 and SMB2 are the customers sharing Shared Tenant 1. They each have one ESAv and one WSAv devices configured, but notice that the IP addresses are the same as Shared Tenant1 ESAv and WSAv devices.

![Sample HSS Device Configuration](image)

Provisioning Workflow

There has been a paradigm shift in the recommended provisioning workflow for Cisco devices with UBIqube MSActivator. UBIqube MSActivator has evolved from using template libraries for device management to their newer object-based support for service management. Most Cisco virtual security appliances are supported with object libraries. A flexible framework is available for additional objects that may be needed, or if customized objects are needed.

Cisco recommends that template configurations be created for initial provisioning. These template configurations can be captured and saved with the UBIqube MSActivator Change Management capability. For each Day 0 device configuration, it is best to use the native web management support to create it. For the Day 0 configuration for the ASAv, Cisco recommends either using ASDM or referring to Appendix D—HSS Enterprise Designs Tested, page 113 for the configuration that was tested with this update. For the WSAv and ESAv Day 0 configuration, use the web GUI to create the initial Day 0
configuration.

For Day 1+ configuration, the configurations can then be altered to be customer specific and have their service delivery tiered as desired with the UBIQube MSActivator Service management capability.

During initial provisioning there is template support for SNMP and Syslog support to tailor for device specific settings. After that provisioning based on objects in service provisioning is recommended.

Creating the Service Tiers

For each Cisco virtual security appliance there is a corresponding object library in the Repository. To implement service tiers, a service provider administrator would select the objects to tier the service and attach those objects to the devices in the service. Additionally, the service provider administrator may choose to allow end customers the ability to provision their service via the customer portal.

This section describes the service tier examples for both the ESA and WSA. Both the ESA and WSA appliances are policy provisioned by creating/modifying the XML configuration file. When ESA and WSA devices are created with UBIQube MSActivator, a configuration is applied to the device that is used to provision the initial policy.

For all Cisco virtual security appliances, it is assumed that VMware vCenter has provisioned a virtual machine for the security virtual appliance that has the correct number of cores, memory, and disks. 

Table 20 lists the service tier examples for the ESAv. Tier 1 is provisioned as the Day 0 configuration. When creating service tiers 2–4, Cisco recommends using MSActivator Service Management to create the service tiers.

<table>
<thead>
<tr>
<th>Service Tier</th>
<th>SenderBase Reputation Scoring</th>
<th>Anti-Spam</th>
<th>Local Anti-Spam Quarantine</th>
<th>Outbreak Filters, Sophos Anti-Virus</th>
<th>Content Filters</th>
<th>External Load Balancing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>optional</td>
</tr>
</tbody>
</table>
Figure 53 shows the ESA object library in the Repository. The objects are highlighted in RED.

**Figure 53  Repository Files for Cisco ESA**

![Image of Cisco ESA object library](https://example.com/image.png)

Table 21 lists the ESA object library elements in the HSS ESA Object Library. There are two folders in the ESA Object Library: HSS_Common and HSS_SMB. HSS_Common objects are used on Enterprise and Shared Tenant customers. These objects set up the common policy for the ESA device. HSS_SMB contains objects that are applicable to SMB customers that use the Shared Tenant to provide email security.

**Table 21  ESA Object Library Elements**

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Element Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSS_Common Folder: Antispam.xml</td>
<td>To enable/disable antispam support, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Antivirus.xml</td>
<td>To enable/disable antivirus support, add this object to the ESA configuration.</td>
</tr>
</tbody>
</table>
The above objects can be copied into the Object Operator area to create various service tiers. Some sample service tiers have been created for Bronze and Silver service tiers. The first step is to attach the objects to the Enterprise 1 ESAv device, as in Figure 54. Select Attach Files highlighted in Red.

<table>
<thead>
<tr>
<th>Table 21</th>
<th>ESA Object Library Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSS_Common Folder: Content_Filter_In.xml</td>
<td>To enable/disable content filters, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: LDAP.xml</td>
<td>To set up LDAP Server Profiles, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Mail_Policy_in.xml</td>
<td>To set up the inbound mail policy, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Mail_Policy_in_DEFAULT.xml</td>
<td>To set up the default inbound mail policy, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Outbreak_filter.xml</td>
<td>To enable/disable outbreak filters, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: RAT.xml</td>
<td>To set up the Recipient Access Table (RAT), add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: SMTP_Route.xml</td>
<td>To set up the SMTP Route, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: SNMP.xml</td>
<td>To enable SNMP monitoring by MSActivator, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Senderbase_Status.xml</td>
<td>To enable Sender-based reputation scoring, add this object to the ESA configuration.</td>
</tr>
<tr>
<td>HSS_SMB Folder: Content_Filter_In_customerFiltered.xml</td>
<td>For use with a shared ESA deployment, this object sets up the customer-specific incoming content filters.</td>
</tr>
<tr>
<td>HSS_SMB Folder: Mail_Policy_in_customerFiltered.xml</td>
<td>For use with a shared ESA deployment, this object sets up the customer-specific incoming mail policy.</td>
</tr>
</tbody>
</table>
Figure 54    Attach Objects to Ent1 ESAv
The next step is to select the green plus sign that is highlighted in Red to navigate to the objects to be attached, as in Figure 55.

**Figure 55  Select Attached Objects**

The next step is to navigate to the SPA operator area and select the sample HSS_Enterprise_Service_Tier_Silver and then select OK, as in Figure 56.

**Figure 56  Select the HSS Enterprise Service Tier Silver Set of Objects**
The last step is to save the objects selected to the ESAv device instance, select Save, which is highlighted in Red in Figure 57.

Figure 57  **Save ESAv Objects to Ent1 ESAv**

![Image of Save ESAv Objects to Ent1 ESAv](image1.png)

Figure 58  **Service Management of Ent1 ESAv on Config Tab**

![Image of Service Management of Ent1 ESAv on Config Tab](image2.png)
Table 22 lists the service tier examples for the WSAv.

Table 22  WSAv Service Tier Examples

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>optional</td>
<td>optional</td>
</tr>
<tr>
<td>2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>optional</td>
<td>optional</td>
</tr>
<tr>
<td>3</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>optional</td>
<td>optional</td>
</tr>
<tr>
<td>4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>optional</td>
<td>optional</td>
</tr>
<tr>
<td>5</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>optional</td>
<td>optional</td>
</tr>
<tr>
<td>6</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>optional</td>
<td>optional</td>
</tr>
</tbody>
</table>

Figure 59 shows the WSA object library in the Repository. The objects are highlighted in RED.

Figure 59  Repository Files for Cisco WSA
Table 23 lists the WSA object library elements in the HSS WSA Object Library. There are two folders in the ESA Object Library: HSS_Common and HSS_SMB. HSS_Common objects are used on Enterprise and Shared Tenant customers. These objects set up the common policy for the WSA device. HSS_SMB contains objects that are applicable to SMB customers that use the Shared Tenant to provide web security.

Table 23  WSA Object Library Element

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Element Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSS_Common Folder: Access_PoliciesGroups_customOnly.xml</td>
<td>To enable/disable URL Filtering and Application Visibility Control, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Authentication_LDAP.xml</td>
<td>To set up user authentication to the tenant’s LDAP server, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Authentication_NTLML.xml</td>
<td>To set up user authentication to the tenant’s NTLML server, add this to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_Custom_URL_Categories.xml</td>
<td>To set up custom URL categories, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_dns_servers.xml</td>
<td>To set up DNS, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_Gateway.xml</td>
<td>To set up the default gateway, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: Identity.xml</td>
<td>To set up identity/authentication policy, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_Malware_Scanning.xml</td>
<td>To enable/disable Sophos or McAfee antivirus support, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_NTP.xml</td>
<td>To set up NTP servers, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_ROUTES.xml</td>
<td>To set up static routes, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_Common Folder: WSA_SNMP.xml</td>
<td>To enable/disable SNMP for UBIqube to monitor the device, add this object to the WSA configuration.</td>
</tr>
<tr>
<td>HSS_SMB Folder: AccessPoliciesGroupsFiltered.xml</td>
<td>To enable/disable shared WSA deployments to delegate access provisioning of the end customer’s access policy, add this object to the WSA configuration.</td>
</tr>
</tbody>
</table>
The above objects can be copied into the Object Operator area to create various service tiers. Some sample service tiers have been created for Bronze and Silver service tiers. The first step is to attach the objects to the Enterprise 1 WSAv device, as in Figure 60. Select Attach Files highlighted in Red.

Figure 60  Attach Objects to Ent1 WSAv
The next step is to select the green plus sign that is highlighted in Red to navigate to the objects to be attached, as in Figure 61.

**Figure 61  Select Attach Objects**

The next step is to navigate to the SPA operator area and select the sample HSS_Enterprise_Service_Tier_Silver and then select OK, as in Figure 62.

**Figure 62  Select the HSS Enterprise Service Tier Silver Set of Objects**
The last step is to save the objects selected to the WSAv device instance, select Save, which is highlighted in Red in Figure 63.

Figure 63  Save WSA Objects to Ent1 WSAv

Figure 64  Service Management of Ent1 WSAv on Config Tab
Figure 65 shows the repository files for Cisco ASA.

**Figure 65**  Repository Files for Cisco ASA
Table 24 lists the ASA Object Library elements in the repository.

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Element Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA folder: ldapServer</td>
<td>To define an LDAP server to authenticate users to.</td>
</tr>
<tr>
<td>AAA folder: localUser</td>
<td>To define authentication credentials for a user.</td>
</tr>
<tr>
<td>FW folder: accessListObject.xml</td>
<td>To define access list objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: accesslist.xml</td>
<td>To define access lists, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: addressObject.xml</td>
<td>To define address objects, add this to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: interfaces.xml</td>
<td>To configure interfaces, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: logObject.xml</td>
<td>To enable syslogs to be sent to UBIqube MSActivator for reporting, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: natRulesObject.xml</td>
<td>To define NAT Rules objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: objectGroup.xml</td>
<td>To define Group objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: rangeObject.xml</td>
<td>To define Range objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: serviceGroup.xml</td>
<td>To define Service Group objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>FW folder: serviceObject.xml</td>
<td>To define Service objects, add this object to the ASA configuration.</td>
</tr>
<tr>
<td>VPN folder: PeerVPN</td>
<td>To define the Site to Site Peer VPN.</td>
</tr>
<tr>
<td>VPN folder: RemoteAccessVPN</td>
<td>To define the Remote Access VPN Policy.</td>
</tr>
<tr>
<td>VPN folder: access_list</td>
<td>To define the VPN access-list</td>
</tr>
<tr>
<td>VPN folder: anyconnectimage</td>
<td>To define the anyconnect image to be used for remote access.</td>
</tr>
<tr>
<td>VPN folder: ikev1Policy</td>
<td>To define the IKE v1 policy.</td>
</tr>
<tr>
<td>VPN folder: ikev1TransformSet</td>
<td>To define the IKEv1 transform set.</td>
</tr>
</tbody>
</table>
Figure 66 shows the service management of ASAv objects.

**Figure 66 Service Management of Ent2 ASAv Config Tab**

<table>
<thead>
<tr>
<th>VPN Folder: ikev2Policy</th>
<th>To define the IKE v2 policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Folder: ikev2Proposal</td>
<td>To define the IKE v2 proposal.</td>
</tr>
<tr>
<td>VPN Folder: trustpoint</td>
<td>To define the VPN trustpoint.</td>
</tr>
</tbody>
</table>
Figure 67 shows the repository files for Cisco CSR1000v.

Figure 67  Repository Files for Cisco CSR1000v

Table 25 lists the CSR1000v Object Library elements in the repository.

Table 25  CSR1000v Object Library Elements

<table>
<thead>
<tr>
<th>Element Name</th>
<th>Element Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW folder: access_list</td>
<td>To define access lists, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW folder: address</td>
<td>To define address objects, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW folder: firewall_policy</td>
<td>To define firewall policy, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW folder: interface</td>
<td>To configure interfaces, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW folder: logObject.xml</td>
<td>To enable syslogs to be sent to UBlqube MSActivator for reporting, add this object to the CSR1000v configuration.</td>
</tr>
</tbody>
</table>
Table 25  **CSR1000v Object Library Elements (continued)**

<table>
<thead>
<tr>
<th>Folder</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW</td>
<td>service</td>
<td>To define a service, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW</td>
<td>static_route</td>
<td>To define a static route, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>FW</td>
<td>vrf.xml</td>
<td>To define a VRF, add this object to the CSR1000v configuration.</td>
</tr>
<tr>
<td>VRF</td>
<td>vrf_to_int.xml</td>
<td>To define a VRF on an interface, add this object to the CSR1000v configuration.</td>
</tr>
</tbody>
</table>

**Figure 68** shows the service management of CSR1000v objects.
UBIQube MSActivator Common Operations

This section provides an overview of common UBIqube MSActivator Operations that need to be performed to do multi-tenant security domain management of any device that UBIqube MSActivator supports.

Common operations are as follows:
- Creating delegation profiles
- Creating managers
- Creating devices

The HSS demo including UBIqube MSActivator is available on the Cisco demo cloud [https://dcloud.cisco.com](https://dcloud.cisco.com). Contact your Cisco account team if interested in having this demo activated for your account.
Creating Delegation Profiles

You need to create delegation profiles that define the end customer level of access policy. In general, there are usually two levels for end customer manager accounts: End Customer Monitors Only access and End Customer Admin access. It is best to decide in advance all the required access levels across all the end customers to configure a set of standard delegation profiles. Then, as customers are created in MSActivator you can create the managers and apply the appropriate delegation profile.

Procedure

Step 1 Log in as the SP privileged administrator. SPA-Admin is an example administrator. (See Figure 69.)
Step 2  Click **Delegations** to display the current delegations. Click the Green plus sign to add a new delegation profile. (See **Figure 70**.)

**Figure 70  Create a Delegation Profile**
Step 3  To create a delegation profile start on the Managed Devices Tab. Enter the delegation profile name SMB-readwrite for the SMB Administrator delegation profile. Select the change management View box, select the Object Management Manage box, and Service Management Manage box. Select the Customer Tab to continue setting up the delegation profile. (See Figure 71.)

Figure 71  Delegations – Managed Devices Tab
Step 4  Select the change management View box. Select the Portal Tab to continue setting up the delegation profile. (See Figure 72.)

Figure 72  Delegations – Customer Tab

Step 5  Select the Customer Access and View asset boxes. Save the delegation profile. (See Figure 73.) This delegation profile allows all SMB managers to change configuration policy in addition to the default monitoring features.

Figure 73  Delegations – Portal Tab
Creating Managers

After you create the delegation profiles follow these steps to create the managers.

Procedure

Step 1  Log in as the SP privileged administrator. SPA-Admin is an example administrator. (See Figure 74.)

Figure 74  Login
Step 2  Click the Managers Tab, and then select the man with the plus sign in the upper right hand corner highlighted in Red. (See Figure 75.)

Figure 75  Managers Tab—Create Manager

Step 3  Click the Manager Entity type highlighted in Red (See Figure 76.)

Figure 76  Select Manager Entity Type
**Step 4**  
On the Domain tab, attach this manager to the customer. (See Figure 77.)

*Figure 77  Create Manager—General Tab*

**Step 5**  
Click Save to complete setting up the manager account. (See Figure 78.)

*Figure 78  Create Manager—Domain Tab*
Creating Devices

The following sample workflow shows how to create a device in MSActivator for the ESAv or WSAv.

Procedure

**Step 1** Log in as the SP privileged administrator. SPA-Admin is an example administrator. (See Figure 79.)

![Login](image-url)
Step 2  Select customer Enterprise 2 and select the plus sign highlighted in Red to add a device (see Figure 80.)
**Solution Validation**

**Step 3** Select Manufacturer Cisco and Model WSA highlighted in Red. (See Figure 81.)

*Figure 81 Select Cisco WSA Device*

**Step 4** Fill in the information in Red in the Simple or Expert Device configuration and then select **Save**, as shown in Figure 82 and Figure 83.

*Figure 82 Simple Device Configuration*
Figure 83  Expert Device Configuration
Step 5  Select the Attach Files icon highlighted in Red. (See Figure 84.)

Figure 84  Attach Files
Step 6 Select the Ent2 WSA Day 0 configuration from the operator area of the repository, and click OK. (See Figure 85.)

Figure 85 Attach Ent2 WSA Day 0 Configuration

Step 7 Accept the imported configuration. (See Figure 86.)

Figure 86 Accept Ent2 WSA Day 0 Configuration
**Solution Validation**

**Step 8**  
Save the configuration. (See Figure 87.)

**Figure 87**  
**Save Ent2 WSA Day 0 Configuration**

**Step 9**  
Select initial provisioning, highlighted in Red. (See Figure 88.)

**Figure 88**  
**Initial Provisioning**
**Step 10** It can take a few minutes for the process to complete. Check back and confirm that the configuration was updated (see Figure 89) by referring to the time stamp highlighted in Red.

**Figure 89** Confirm Device Created and Configuration Updated
SMB Design Guidance

For SMB Designs, the following is the required workflow to enable the multi-tenancy capability for customer portal service management available with MSActivator for the WSAv and ESAv.

**Step 1** Create a Customer called “Shared Tenant 1”.

**Step 2** Create devices under Shared Tenant 1 for CSR1000v, WSAv, and/or ESAv (see Figure 90).

**Figure 90**  
Shared Tenant 1 Example

---

**Step 3** Attach Day 0 configuration, and perform initial provisioning for each of the devices.

**Step 4** Attach objects from the HSS_Common folder to devices WSAv and ESAv and for CSR1000v add objects from the ISR (CSR) object library for service provider service management of the devices for the shared tenant.
Step 5  Create a Customer for each SMB customer; SMB1 and SMB2, for example.

Step 6  For each SMB customer, create a device for ESAv called “Email Security Service” and use the same IP address as the ESAv in Shared Tenant 1.

Step 7  For each SMB customer, create a device for WSAv called “Web Security Service” and use the same IP address as the WSAv in Shared Tenant 1.

The following figures for SMB1 and SMB2 show a sample configuration.

Figure 91  Customer SMB1 Services Example
Step 8  For each SMB customer, create login accounts for the end customer with the preferred delegation profile: SMB1-Admin, SMB1-Monitor, SMB2-Admin and SMB2-Monitor, for example.
Step 9  Attach HSS_SMB objects to the device under each of the SMB customers. SMB objects are in the HSS_SMB folder in the WSAv and ESAv object repository (see Figure 93 and Figure 94).

Figure 93  Attach HSS_SMB Objects to SMB1

Figure 94  Save HSS_SMB Objects to SMB1
Step 10  Currently the new customer portal does not support the ability to create a configuration variable. You must go to the MSActivator Legacy Portal (Figure 94) to create the configuration variable needed for SMB designs. In the SP legacy portal at Customer level navigate to each SMB customer (Figure 95) add a configuration object CUSTOMER_REF=SMBn where “n” is specified uniquely for each of the SMB customers, (see Figure 97, Figure 98 and Figure 100).

Figure 95  MSActivator SP Legacy Portal

Figure 96  SMB Customers
Figure 97  Customer Level: Edit Configuration Variables Tab

Figure 98  Add a Configuration Variable

Figure 99  Add Configuration Variable CUSTOMER_REF Example
Step 11 Return to the new customer portal navigate to customer SMB1 and perform service management on just SMB1 specific policy.

Figure 100 Service Management SMB1 Example
Concluding Remarks

This guide describes the design topology and provides design guidance for the Cisco Hosted Security as a Service Solution for next generation firewall, firewall, VPN, web and email security services. Consult the references in Appendix A for more detailed information on products included in this design.

About the Authors

Albra Welch, Security Solutions Architect, Security Business Group, Cisco

Albra is currently the HSS Lead Architect and is focused on Service Provider Security Solutions. Albra has held various senior technical roles including: VXI Systems Architect, TrustSec Solution Manager and Architect, MACsec Partner Relationship Manager, IOS VPN Technical Leader, and uBR925 Cable Modem Software Project Leader.

Peter Dowker, Security Solutions Architect, Security Business Group, Cisco

Peter Dowker has worked at Cisco Systems as Consulting Systems Engineer, Systems Engineer, Manager, Systems Engineering and Content Security Solutions Architect in the Service Provider, Enterprise and Government sectors.
Appendix A—References

- Cisco Firepower NGFW Data Sheet—

- Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide—

- Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide—

- Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide—

- ASAv At a Glance—

- ASAv Datasheet—

- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.4—

- ASDM Book 3: Cisco ASA Series VPN ASDM Configuration Guide, 7.4—

- AnyConnect configuration file information—

- Cisco IOS CA support information—

- WSAv—

- ESAv—

- UBiqube—
  http://www.ubiqubesolutions.com

- Cisco Powered Cloud and Managed Services Program—

- Cisco AMP Threat Grid—

- Cisco AMP Virtual Private Cloud—

- Virtual Services Architecture—

- Virtual MultiService Data Center Architecture—
  http://www.cisco.com/go/vmdc
Appendix B—ESA High Availability Design Considerations

When designing the ESA system architecture, the SP should observe these general principles of high availability engineering:

- Elimination of single points of failure—This means adding redundancy to the SP data center so that component failure does not produce an entire system failure.
- Reliable failover—In multi-tiered multi-host network based systems, the failover point itself can become a single point of failure. High availability engineering must provide for reliable failover between multiple SP data centers.
- Detection of failures as they occur—Providing that the two principles above are observed, an end user should never experience a failure. At the same time, the SP operation must detect and track component failures when they happen.

When deploying the Cisco ESA in a multiple instance scenario, SPs should observe the following high availability best practices:

- Direct Server Return
- DNS Round Robin
- ESA Clustering
- External Load Balancers

Direct Server Return

Direct Server Return (DSR) is a method that supports light-weight load balancing between multiple ESA appliances that share the same virtual IP address.

When enabling DSR, the following rules apply:

- All appliances use the same VIP address
- All appliances must be on the same switch and subnet as the load balancer

To enable DSR on the ESA appliance, follow these steps:

**Procedure**

**Step 1** Enable the “loopback” Ethernet interface on each participating appliance.

```
mail3.example.com> etherconfig
```

a. Choose the operation you want to perform:
   - MEDIA—View and edit ethernet media settings
   - PAIRING—View and configure NIC Pairing
   - VLAN—View and configure VLANs
   - LOOPBACK—View and configure loopback

```
[1]> loopback
Currently configured loopback interface:
```

b. Choose the operation you want to perform:
   - ENABLE—Enable loopback interface
[]> enable
Currently configured loopback interface:
1. Loopback
c. Choose the operation you want to perform:
   - DISABLE—Disable Loopback Interface

[]>
d. Choose the operation you want to perform:
   - MEDIA—View and edit ethernet media settings
   - PAIRING—View and configure NIC pairing
   - VLAN—View and configure VLANs
   - LOOPBACK—View and configure loopback

[]>

**Step 2** Create an IP interface on the loopback interface with a virtual IP address.

mail3.example.com> interfaceconfig
Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. Management (10.10.0.10/24: example.com)
a. Choose the operation you want to perform:
   - NEW—Create a new interface
   - EDIT—Modify an interface
   - GROUPS—Define interface groups
   - DELETE—Remove an interface

[]> new
b. Enter a name for this IP interface (Ex: “InternalNet”):

[]> LoopVIP
IP Address (Ex: 10.10.10.10):
[]> 10.10.1.11
Ethernet interface:
1. Data 1
2. Data 2
3. Loopback
4. Management
5. VLAN 31
6. VLAN 34

1]> 3
Netmask (Ex: "255.255.255.0" or "0xffffffff00"):
[255.255.255.0]> 255.255.255.255
Hostname: []> example.com

Note: The Loopback interface configuration requires a /32 or all 1’s subnet mask to avoid an overlap with the physical adapter subnet address.

Do you want to enable FTP on this interface? [N]>
Do you want to enable Telnet on this interface? [N]>
Do you want to enable SSH on this interface? [N]>
Do you want to enable HTTP on this interface? [N]>
Do you want to enable HTTPS on this interface? [N]>

Currently configured interfaces:
1. Data 1 (10.10.1.10/24: example.com)
2. InternalV1 (10.10.31.10/24: mail31.example.com)
3. LoopVIP (10.10.1.11/24: example.com)
4. Management (10.10.0.10/24: example.com)

Choose the operation you want to perform:
- NEW—Create a new interface
- EDIT—Modify an interface
- GROUPS—Define interface groups
- DELETE—Remove an interface

[]>
mail3.example.com> commit

**Step 3** Create a listener on the new IP interface. You can do this through the `listenerconfig` command in the CLI or through the **Network > Listeners** page in the GUI.

**Step 4** Commit all changes to complete the configuration.

**DNS Round Robin**

When end user organizations are sending and receiving a large volume of email messages, the SP can add multiple ESA appliances to help manage the load and to avoid queues and deliver delays. When using multiple ESAs, the SP can route the inbound email to multiple MTAs so that the appliances will process roughly the same volume of email, thus load balancing the mail servers.

The following are two possible scenarios for load balance mail servers or MTAs by using DNS:
- Define multiple MX records with the same priority
- Define multiple A records with the same name and different IP addresses
**MX Records, DNS and Email Routing**

A Mail exchanger (MX) record is a type of resource record in the Domain Name System (DNS) specifying how Internet email should be routed by using the Simple Mail Transfer Protocol (SMTP). DNS provides a lookup of domain names to IP addresses. MX records are a type of DNS record that identifies the IP address(es) responsible for a particular domain.

The MX record typically returns the Fully Qualified Domain Name (FQDN) of the mail server(s). For example, when a DNS query for the MX records of yourcompany.com is made, you will get two FQDNs: esa1.yourdomain.com and esa2.yourdomain.com. DNS then translates the FQDNs to an IP address that the sending mail servers use for sending emails.

**Define Multiple MX Records with the Same Priority**

In this case, the manager of the customer DNS MX records are defining 2 MX records with an equal value.

The example shows that the two records have an equal MX preference of 10. When using this method, the DNS server returns both MX records and their respective associated IP addresses. The sending MTA (mail server) selects one IP address based on its algorithm and uses it to deliver the mail.

<table>
<thead>
<tr>
<th>Record FQDN</th>
<th>Record Type</th>
<th>MX Preference</th>
<th>Record Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>yourdomain.com</td>
<td>MX 10</td>
<td>mail1.yourdomain.com</td>
<td></td>
</tr>
<tr>
<td>yourdomain.com</td>
<td>MX 10</td>
<td>mail2.yourdomain.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(IP addresses resolved below)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail1.yourdomain.com</td>
<td>A 10.0.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mail2.yourdomain.com</td>
<td>A 10.0.0.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Define Multiple A Records with the Same Name and Different IP Addresses**

When using the second method, the IP addresses of the mail servers are defined in A records with the same name. The A record is configured as the FQDN in the MX record. The sending mail server sends the email to the first IP address in the list. (The SP might need to configure end user records on the authoritative DNS server to provide the IP addresses in a random order.)

<table>
<thead>
<tr>
<th>Record FQDN</th>
<th>Record Type</th>
<th>MX Preference</th>
<th>Record Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>yourdomain.com</td>
<td>MX 10</td>
<td>mail.yourdomain.com</td>
<td></td>
</tr>
<tr>
<td>yourdomain.com</td>
<td>MX 10</td>
<td>mail.yourdomain.com</td>
<td></td>
</tr>
<tr>
<td>mail.yourdomain.com</td>
<td>A 10.0.0.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A 10.0.0.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Limitations of MX Records**

Using MX records for failover and redundancy has some drawbacks. These are a few reasons why MX records might not be adequate for your system architecture:

- MX records cannot provide for fractional load splitting—Client behavior is to choose from equal-priority MX hosts at random. For example, if you have two records at an MX cost of 10, each will see half of the traffic; if you have three, each will see a third, and so on. If you want one server to receive 50% of the traffic and two other servers to receive 25%, or other unequal splits, MX records cannot solve that problem.
• MX records are more difficult to use for load balancing outbound mail to Microsoft Exchange smart hosts.

• MX records require individual hosts—This means that each host must have its own public IP address, DNS A and PTR records, and possibly its own TLS certificate. Adding new hosts to the MX list might require allocation of new IPs, changes to DNS, and purchasing a certificate from a root certificate authority (CA).

• Load balancing between multiple hosts with equal priority isn’t perfect—Because SMTP clients use varying techniques to determine how to choose among equally weighted records, loads may be slightly higher on any one host. Typically, the difference is not high enough to worry about but there could be about 5% more connections to one server than the others.

• MX records are generally static—Like all DNS resource records, MX and A records for mail servers have a Time to Live (TTL) that varies. It is typically no shorter than one hour and often much longer, as much as one day or more. It is possible to make MX TTLs shorter, but even if this is done, many SMTP clients might not honor the shorter TTL. The TTL problem presents operational challenges if you need to quickly add or remove systems from your environment.

• Avoid having too many hosts in your MX records that can cause DNS resolution problems—DNS as a protocol requires both UDP and TCP, but UDP is used for the vast majority of responses. When the response is larger than the maximum UDP DNS payload limit of 512 bytes, DNS switches to TCP. In many environments, the use of TCP by DNS is not understood, and firewalls block the port 53 TCP connection.

   The result is that the MX record appears not to exist, and email can’t be delivered. The issue lies with the client’s DNS environment. But of course, when email can’t be delivered to your servers, it’s your problem.

   Most email domains on the Internet today load balance through the use of MX records. It is likely that even after the transition to IPv6, MX records will continue to be the leading approach to load balancing and failover among mail servers. If the limitations of MX records are problematic for your environment, consider hardware or software load balancers.

### ESA Clustering

The SP can configure customer instances of the Cisco ESA appliances in a cluster. Clustering ESA appliances allows the devices to share common services, common policies, and to propagate policy configuration changes across all cluster members. Cluster communications occur between devices in a peer to peer architecture on either port 22 (SSH) or 2222 (Cluster Communication Service). ESA clusters can exist across VLANs, routes or geographic boundaries because each cluster member manages its own SMTP sessions and messages. Note however, ESA clusters do not provide load balancing capabilities or an active/standby configuration.

Not every configuration can be shared across all appliances in the cluster. The purpose of clustering is to provide a working configuration on all appliances and to avoid duplication. Some configurations are appliance specific and therefore are configured on machine level. (Settings on this level are the IP address, the hostname, and the default gateway. Typically, any configuration that could cause issues when active on all appliances must be installed at the machine level.)

All other configuration policies and variables such as LDAP profiles and queries, Listeners, SMTP routes, content filters, mail policies, etc) can be shared across cluster members and should not be applied on machine level. (They can be applied to either group or cluster level.)

The cluster level is the top level of administration and represents all appliances connected in the cluster. The group level can be established as a sub level of the cluster to organize appliances in the same location, or for the same purpose. For example inbound traffic versus outbound traffic, Europe
versus US location, etc.
The group level is optional and by default not present when initializing the cluster. Configuration changes performed at the group level affect only the appliances that are members of the group.
Clustering is covered in depth in Chapter 8 of the Cisco IronPort AsyncOS 7.6 for Email Advanced Configuration Guide. Please read all relevant documentation regarding the product and its capabilities before beginning configuration.

External Dedicated Load Balancers

Dedicated software or hardware load balancers can offer an attractive alternative to using multiple MX records for the SP. Load balancers spread the connection load based on connection count, connection history, ESA system load, and other attributes instead of sender behaviors. Load balancers can also direct traffic unevenly—for example, dividing the load across four ESAs in a 30/30/20/20 spread instead of the 25/25/25/25 spread that would result from four hosts in an MX record. This is ideal if you have different models or sizes of ESA, or SP data centers with varying throughput capabilities.

Making changes to a load balanced environment is typically faster than dealing with MX records. This is because there are no DNS caching issues when you remove an ESA from the load balance pool.

Deploying ESAs is similar to a standard deployment with a load balancer. The real IPs of the ESAs are not used in the MX records or smarthost settings. Instead, the SP should publish an MX record with a hostname that resolves to a virtual IP address on the load balancer:

```
yourdomain.com.  86400 IN  MX  10 inbound.yourdomain.com
```

The virtual IP address then distributes the connections to the internal real IPs of the ESAs.

Load Balancers for Inbound Mail

Load balancers for inbound mail do not provide any new capabilities over MX record hosts, but they do provide the SP with more deployment flexibility.

Configuring load balancing for ESA is much like configuring load balancing for any other server application. It should be either round-robin SMTP connections, or a least-load connection algorithm. Simple load balancers use only connection count to determine where to send the next connection. If the SP has more advanced capabilities such as health checks or SNMP polling, these can use the ESA CPU usage and work queue count attributes to determine the least-load ESA.

Caution

In all cases, do not use any type of source Network Address Translation (NAT). The ESAs require that the originating IP of the client is preserved in the TCP connection to perform accurate SenderBase reputation lookups.

Per-host rate limiting and other sender controls also depend heavily on the true source IP being preserved on inbound connections.

For inbound connections from Internet SMTP clients, Cisco recommends using load-balancer stickiness features, if available, to send repeated connections from the same source IP to the same destination ESA. This allows the ESA rate limiting to properly count individual clients and to rate limit appropriately. Pure round-robin results in each ESA enforcing its own limits and bad senders enjoying higher connection rates than they would have otherwise.

If the SP elects to use simple port 25 SMTP health check probes on the load balancer, make sure the connecting IP is granted a generous HAT policy on the ESAs. Otherwise, you run the risk of rejecting or rate limiting the connections and forcing the load balancer to drop the ESA out of the pool.
The ESA configuration is not much different from any other deployment. For simplified troubleshooting, it’s important to synchronize all the ESA configurations in a load-balancer pool. It can be maddening to track down a configuration problem when it’s only affecting some of your email messages or connections. You’ll even want to keep hostnames the same across the appliances to maintain the illusion of a single large host. Each ESA can maintain its own unique global hostname so that it can be distinguished. The hostname assigned to the load-balanced real IP on each ESA should be identical and it should match the external hostname of the virtual IP address.

For example, if Yourdomain.com is using this MX record:

```
yourdomain.com. 86400 IN MX 10 inbound.yourdomain.com
```

It resolves to this IP address:

```
inbound.yourdomain.com. 86400 IN A 128.107.234.204
```

This is a virtual IP address that is prefixed in four individual ESAs:


All four ESAs should have a configuration that looks like this output from the interfaceconfig command prompt:

Currently configured interfaces:

1. data (10.1.42.42/24 on Data 1: inbound.cisco.com)

Choose the operation you want to perform:

- NEW—Create a new interface
- EDIT—Modify an interface.
- GROUPS—Define interface groups.
- DELETE—Remove an interface.

Keeping all four of the interface hostnames identical means that each ESA will use the same banner hostname during SMTP. This is true for TLS certificates and certificate verification, and for SPF verification of HELO domains.

### Load Balancers for Outgoing Mail

The use of load balancers is especially appropriate for outgoing email. This is at the point in the architecture where end users groupware or mail store servers deliver messages to the ESAs for Internet destinations. Most groupware servers have the ability to send messages to a “smarthost” that accepts email to all nonlocal recipients. The smarthost setting is often limited to a single hostname or IP address, or to a list of hosts that have simple round-robin load balancing. For some systems, there is no load-balancing support for smarthosts.

It is possible to use MX records for load balancing and failover of smarthosts. However, this requires that the customer DNS administrator or SP publish a wildcard DNS entry for all nonlocal domains, with the host records resolving to the ESA IP addresses. Any end customers internal system needing to send email to an Internet destination does its own MX record lookup for the destination domain. The DNS server always returns the same values regardless of the domain:

```
gmail.com. 86400 IN MX 10 esa1.yourdomain.com
```

```
gmail.com. 86400 IN MX 20 esa2.yourdomain.com
```
Configuration of a load balancer itself is beyond the scope of this document although many of the
guidelines applied to incoming SMTP load balancing also apply to outgoing. For example:

- Load balance based on least-load or round-robin of connections—If the load balancer offers health
cHECKS or other load determination features based on SNMP, you should use them. At a minimum,
the SP should use port 25 health checks. On the ESA, the SP must whitelist the load balancer health
check IPs to avoid rejecting or rate limiting these health check connections.

- Do not use source NAT on connections from internal hosts—The ESA needs to see the connections
FROM individual hosts in order to apply connection and rate limits on a per-host basis. NAT prevents
the ESA from the ability to distinguish individual internal hosts.

- Load balancers operate by rewriting destination IPs that make it appear as if the client and server
are directly communicating—To avoid asynchronous TCP connections, and to maintain original
source IPs, the internal groupware and smart host ESAs should be on different subnets. Ideally, the
ESAs should be separated into their own subnet.

For example, an Exchange server has IP 10.10.17.23/24, and there are three ESAs at
10.10.17.130–132/24. The load balancer virtual IP address is 10.10.17.129. If the Exchange server
initiates an SMTP connection to the load balancer VIP, the load balancer rewrites the destination IP to
that of one of the ESAs. The ESA at 10.10.17.130 recognizes that the Exchange server is on the same
subnet and replies directly thus creating an asynchronous path. The Exchange server drops the return
packets. Moving the virtual IP address to a different subnet will not resolve the issue because the ESA
will continue to reply directly to the Exchange server.

One solution is to separate the ESA from the Exchange server by changing the network settings, or by
splitting the /24 network into at least two subnets. Another solution is to source NAT the Exchange
server. This prevents the ESA from being able to distinguish from multiple internal hosts.
Appendix C—VMDC 2.3 Design Considerations

Figure 101 shows the Cisco VMDC 2.3 Expanded Gold Container Topology.

These are the changes required to accommodate Cisco HSS in a VMDC 2.3 Expanded Gold Container:

- The remote access VPN was moved and attached to the customer private context firewall instead of the customer DMZ context firewall. This was required so that WSAv could support users connecting from the customer site and also through remote access VPN. Because we recommend configuring Web Cache Communication Protocol (WCCP) Redirect on the customer DMZ context firewall, the remote access VPN was attached to an alternative firewall for proper traffic flow.

- Firewall policy and routing to allow access from the customer site to the Internet required the following:
  - Injection of default routes into the customer site that pull traffic into the private zone.
  - Firewall policies that allow access from the customer site to the DMZ.
  - Static routes for customer site subnets on firewalls in both private and DMZ contexts along with injected static routes in the tenant virtual routing and forwarding (VRF) tables.
  - Firewall policies to allow for forwarding of SMTP and DNS queries.
  - WCCP Redirect on the firewall in the customer DMZ context.

- The ESAv location is in DMZ 1 VLAN of the tenant container that is connected to the customer DMZ VRF on the M1 interface. Single NIC mode is recommended for simplicity. The default gateway is the customer DMZ firewall.

- The WSAv location is in DMZ 2 VLAN of the tenant container that is connected to the tenant service VLAN on the M1 interface. Single NIC mode simplifies connectivity to both the tenant Active Directory and the service provider management. A static route is required on the WSAv to the UBIqube MSActivator. The default gateway points to the customer DMZ firewall.
• UBIqube MSActivator connectivity is required through a shared Cisco Adaptive Security Appliance (ASA) context that must be reachable by each tenant container. Network Address Translation (NAT) is used to map ASA/v/WSAv/ESAv IP addresses to a unique IP address in the service provider cloud administrator context. This requirement is because there might be overlapping addresses used across tenant containers.

Figure 102 shows the VMDC 2.3 Expanded Gold Container with HSS.
Appendix D—HSS Enterprise Designs Tested

Enterprise Design 1b—ASAv, ESAv, WSAv, Public AMP, Public Threat Grid

Figure 103  Design 1b—ASAv, ESAv, WSAv, Public AMP, Public Threat Grid

Design 1

[Diagram of Design 1 with network details]

- ASR 9000 dc01-asr9k
- Gold L3VPN GE0/6 10.13.105.1/24
- Gold Internet GE0/7 10.13.8.13/23
- IP SLA
- Management M0/0 10.13.1.112/24
- DMZ GE0/5 10.13.104.1/24
- Gold DMZ GE0/1 10.13.128.32/28
- Gold Management GE0/1 10.13.128.32/28
- Gold Tier 3 GE0/4 10.13.103.1/24
- Gold Tier 2 GE0/3 10.13.102.1/24
- Tier 1 Private Network
- Tier 2 Private Network
- Tier 3 Private Network

Internet
MPLS L3 VPN
ASA Configuration

ASA Version 9.5(2)204

terminal width 511
hostname CU1-ASA1
domain-name cisco.com
enable password <password> encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any6
xlate per-session deny tcp any6 any4
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any6 eq domain
xlate per-session deny udp any6 any4 eq domain

license smart
feature tier standard
throughput level 100M
names
ip local pool VPN 10.13.106.101-10.13.106.150 mask 255.255.255.0

interface GigabitEthernet0/0
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/1
description gold mgnt-dmz
nameif internal-10.13.128.32
security-level 100
ip address 10.13.128.46 255.255.255.240

interface GigabitEthernet0/2
description gold tier1
shutdown
nameif internal-10.13.101
security-level 75
ip address 10.13.101.1 255.255.255.0

interface GigabitEthernet0/3
description gold tier2
shutdown
nameif internal-10.13.102
security-level 75
ip address 10.13.102.1 255.255.255.0

interface GigabitEthernet0/4
description gold tier3
shutdown
nameif internal-10.13.103
security-level 75
ip address 10.13.103.1 255.255.255.0

interface GigabitEthernet0/5
description gold dmz
nameif internal-10.13.104
security-level 75
ip address 10.13.104.1 255.255.255.0

interface GigabitEthernet0/6
description gold l3vpn
nameif l3vpn
security-level 50
ip address 10.13.105.1 255.255.255.0
policy-route route-map wsa-pbr
!
interface GigabitEthernet0/7
description gold internet
nameif internet
security-level 0
ip address 10.13.8.15 255.255.254.0
policy-route route-map wsa-pbr
!
interface GigabitEthernet0/8
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
management-only
nameif Management
security-level 100
ip address 10.13.1.14 255.255.255.0
!
ftp mode passive
dns domain-lookup Management
dns server-group DefaultDNS
   name-server 171.70.168.183
domain-name cisco.com
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network cu3-esa-internal
   host 10.13.104.11
object network cu3-wsa-internal
   host 10.13.104.12
object network cu3-esa-public
   host 10.13.11.31
object network cu3-wsa-public
   host 10.13.11.32
object network VPNClients
   range 10.13.106.101 10.13.106.150
object network VPNPool
   subnet 10.13.106.0 255.255.255.0
description VPNClients
object network cu3-esa-mgmt
   host 10.13.128.36
object network cu3-wsa-mgmt
   host 10.13.128.34
object network cu3-wsa-internal-vip
   host 10.13.104.32
object network cu3-wsa-internal-2
   host 10.13.104.22
object network cu3-wsa2-internal
   host 10.13.104.22
object network cu3-wsa2-mgmt
   host 10.13.128.35
object network internal-10.13.48-network
   subnet 10.13.48.0 255.255.255.0
object network cu3-exch
   host 10.13.48.7
object network cu3-dc
   host 10.13.48.5
description domain controller
Appendix D—HSS Enterprise Designs Tested

object network ubiquue
  host 10.13.1.1
object network ubiquue-nat
  host 10.13.128.36
object network cu3-tier1web
  host 10.13.101.10
object network cu3-tier2web
  host 10.13.102.10
object network cu3-tier3web
  host 10.13.103.10
object-group network INSIDE
  network-object 10.13.101.0 255.255.255.0
  network-object 10.13.102.0 255.255.255.0
  network-object 10.13.103.0 255.255.255.0
  network-object 10.13.104.0 255.255.255.0
object-group network l3vpn
  network-object object internal-10.13.48-network
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq ftp
  port-object eq ftp-data
  port-object eq https
object-group network DM_INLINE_NETWORK_2
  network-object object cu3-wsa-internal
  network-object object cu3-wsa-internal-2
  network-object object cu3-wsa-internal-vip
object-group network DM_INLINE_NETWORK_1
  network-object object cu3-wsa-internal
  network-object object cu3-wsa-internal-vip
  network-object object cu3-tier1web
  network-object object cu3-tier2web
  network-object object cu3-tier3web
object-group network inside-networks
  network-object 10.13.101.0 255.255.255.0
  network-object 10.13.102.0 255.255.255.0
  network-object 10.13.103.0 255.255.255.0
  network-object 10.13.104.0 255.255.255.0
  network-object object internal-10.13.48-network
object-group service DM_INLINE_TCP_3 tcp
  port-object eq ftp
  port-object eq ftp-data
  port-object eq www
  port-object eq https
object-group network DM_INLINE_NETWORK_4
  network-object object cu3-wsa-internal
  network-object object cu3-wsa-internal-2
  network-object object cu3-wsa-internal-vip
object-group service DM_INLINE_NETWORK_3
  network-object object cu3-wsa-internal
  network-object object cu3-wsa-internal-2
  network-object object cu3-wsa-internal-vip
object-group service DM_INLINE_TCP_2 tcp
  port-object eq ftp
  port-object eq ftp-data
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_1
  service-object icmp
service-object tcp destination eq ftp
service-object tcp destination eq ftp-data
service-object udp destination eq snmp
object-group network DM_INLINE_NETWORK_5
  network-object object cu3-es internal
  network-object object cu3-es-public
object-group service DM_INLINE_SERVICE_2
  service-object tcp destination eq domain
  service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_6
  network-object object cu3-es internal
  network-object object cu3-es-public
object-group service DM_INLINE_SERVICE_3
  service-object tcp destination eq smtp
  service-object udp destination eq domain
access-list allow-all extended permit ip object VPNClients any
access-list allow-all extended permit tcp any any eq ftp
access-list allow-all extended permit tcp any any eq ftp-data
access-list allow-all extended permit ip any any
access-list noNat extended permit ip object internal-10.13.48-network object VPNPool
access-list wsa-pbr extended permit tcp 10.13.101.0 255.255.255.0 any eq www
access-list wsa-pbr extended permit tcp 10.13.102.0 255.255.255.0 any eq www
access-list wsa-pbr extended permit tcp 10.13.103.0 255.255.255.0 any eq www
access-list wsa-pbr extended permit tcp 10.13.106.0 255.255.255.0 any eq www
access-list wsa-pbr extended deny tcp any 10.13.104.0 255.255.255.0 eq www
access-list wsa-pbr extended permit tcp 10.13.48.0 255.255.255.0 any eq www
access-list l3vpn extended permit tcp object internal-10.13.48-network object-group DM_INLINE_NETWORK_1 object-group DM_INLINE_TCP_1
access-list l3vpn extended permit tcp object cu3-exch object cu3-es internal eq smtp log default
access-list l3vpn extended deny ip object internal-10.13.48-network object-group inside-networks
access-list l3vpn extended permit tcp object internal-10.13.48-network any object-group DM_INLINE_TCP_3
access-list l3vpn extended permit udp object cu3-dc any eq domain log default
access-list dmz extended permit object-group DM_INLINE_SERVICE_2 object-group DM_INLINE_NETWORK_3 object cu3-dc
access-list dmz extended permit tcp object cu3-es internal object cu3-exch eq smtp log
access-list dmz extended permit object-group DM_INLINE_SERVICE_1 object-group DM_INLINE_NETWORK_4 object ubiquube-nat
access-list dmz extended deny ip any object-group inside-networks
access-list dmz extended permit tcp object-group DM_INLINE_NETWORK_2 any object-group DM_INLINE_TCP_2
access-list dmz extended permit object-group DM_INLINE_SERVICE_3 object cu3-es internal
access-list internet extended permit tcp any object-group DM_INLINE_NETWORK_5 eq smtp log
access-list internal-10.13.102_access_in extended deny ip any
access-list internal-10.13.103_access_in extended deny ip any
access-list internal-10.13.101_access_in extended deny ip any
pager lines 20
logging enable
logging timestamp
logging console debugging
logging buffered informational
logging trap informational
logging history informational
logging asdm informational
logging facility 21
logging device-id string SPA164
logging host Management 10.13.1.81
mtu internal-10.13.128.32 1500
mtu internal-10.13.101 1500
mtu internal-10.13.102 1500
mtu internal-10.13.103 1500
mtu internal-10.13.104 1500
mtu l3vpn 1500
mtu Management 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (internal-10.13.101,internet) source dynamic INSIDE interface
nat (internal-10.13.102,internet) source dynamic INSIDE interface
nat (internal-10.13.103,internet) source dynamic INSIDE interface
nat (l3vpn,internet) source dynamic internal-10.13.48-network interface
nat (internal-10.13.104,internet) source static cu3-esa-internal cu3-esa-public
nat (internet,l3vpn) source static SVN Clients SVN Clients
nat (internet,internal-10.13.104) source static VPN Pool VPN Pool
nat (internet,internal-10.13.103) source static VPN Pool VPN Pool
nat (internet,internal-10.13.102) source static VPN Pool VPN Pool
nat (internet,internal-10.13.101) source static VPN Pool VPN Pool
nat (internal-10.13.104,internal-10.13.128.32) source static cu3-wsa-internal cu3-wsa-mgmt
nat (internal-10.13.104,internet) source static cu3-wsa-internal cu3-wsa-public
nat (internal-10.13.104,internet) source static cu3-wsa-internal-2 cu3-wsa-public
nat (internal-10.13.104,internal-10.13.128.32) source static cu3-esa-internal cu3-esa-mgmt
nat (internal-10.13.104,internal-10.13.128.32) source static cu3-wsa2-internal
cu3-wsa2-mgmt
access-group internal-10.13.101_access_in in interface internal-10.13.101
access-group internal-10.13.102_access_in in interface internal-10.13.102
access-group internal-10.13.103_access_in in interface internal-10.13.103
access-group dmz in interface internal-10.13.104
access-group l3vpn in interface l3vpn
access-group internet in interface internet
!
prefix-list dmz-routes seq 10 permit 10.13.11.0/24 ge 31
!
prefix-list private-routes seq 10 permit 10.13.101.0/24
prefix-list private-routes seq 20 permit 10.13.102.0/24
prefix-list private-routes seq 30 permit 10.13.103.0/24
prefix-list private-routes seq 40 permit 10.13.104.0/24
prefix-list private-routes seq 50 permit 10.13.111.111/32
prefix-list private-routes seq 60 permit 10.13.112.111/32
prefix-list private-routes seq 70 permit 10.13.113.111/32
prefix-list private-routes seq 80 permit 10.13.114.111/32
prefix-list private-routes seq 85 permit 10.13.31.111/32
prefix-list private-routes seq 90 permit 10.13.32.111/32
!
route-map set-nexthop-internet permit 10
!
route-map set-nexthop-l3vpn permit 10
set ip next-hop 10.13.105.254
!
route-map inside-interfaces permit 10
match interface internal-10.13.101 internal-10.13.102 internal-10.13.103
internal-10.13.104
set metric 1000
!
route-map wsa-pbr permit 10
match ip address wsa-pbr
set ip next-hop 10.13.104.32
route-map static-routes-to-bgp permit 10
match tag 1128
set metric 1000

router bgp 65513
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.13.9.254 remote-as 109
neighbor 10.13.9.254 activate
neighbor 10.13.9.254 prefix-list dmz-routes out
neighbor 10.13.9.254 route-map set-nexthop-internet out
neighbor 10.13.105.254 remote-as 109
neighbor 10.13.105.254 activate
neighbor 10.13.105.254 prefix-list private-routes out
redistribute connected route-map inside-interfaces
redistribute static
no auto-summary
no synchronization
exit-address-family

route internet 0.0.0.0 0.0.0.0 10.13.9.254 1
route Null0 10.13.11.31 255.255.255.255 1
route Null0 10.13.11.32 255.255.255.255 1
route Management 64.102.255.40 255.255.255.255 10.13.1.1 1
route Management 171.70.168.183 255.255.255.255 10.13.1.1 1
route Management 173.37.145.8 255.255.255.255 10.13.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h223 0:05:00 h225 1:00:00 mcscp 0:05:00 mcscp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
aaa authorization exec LOCAL
http server enable
http 10.13.1.0 255.255.255.0 Management
snmp-server host Management 10.13.1.81 poll community ubiqube
no snmp-server location
no snmp-server contact
snmp-server community ubiqube
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca certificate policy
auto-import
crypto ca certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
308205ec 308204d4 a0030201 0202106e cc7aa5a7 032009b8 cebcf4e9 52d49130
0d06092a 864886f7 0d010105 05030811 ca110b10 09050355 0405102 05553117
30150603 55040a13 0e566757 6f956757 6e2c2049 6e62e2a1 1f301d00 0555040b
13185665 72653659 676e2054 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303030 56657269 5369676e 0c20496e 06035504 03333c56
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043
65726953 6976e20 436c6173 73203032 5075626c 69632050 72696d61 0e566572
6976e20 436c6173 73203032 0e566572 6976e20 436c6173 73203032 5075626c 69632050 72696d61 72792043

Appendix D—HSS Enterprise Designs Tested

74776f72 6b313b30 39060355 040b1332 5465726d 73206f66 20757365 20617420
68747470 733a2f2f 77772e76 65727369 676e2e63 6f6d2f77 733a2f2f63 726c2e76 657269 736967 6e2f74 74703a2f2f6c 6f672e76 657269 736967 6e2f70 636133 2d67352e 63726c30 060355 1d1f042d 302b3029a027 546f6d2f70 636133 2d67352e 63726c30 060355 1d070100 61305fa1 5da05b30 59305730 55160969 6d616765 2f676966 3021301f 30070605 2b0e0302 1a04148f e5d31a86 ac8d8e6b c3cf806a d448182c 7b192e30 25162368 7474703a2f2f63 662e636f 6d706355 1d200469 306b0686 480186f8 45010717 03030630 28060355 1d230418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0603 551d0e04 1604140d 445c1653 44c1827e 1d200a25 4f0163d8 be79a530 1f060355 1d203418 30168014 7fd365a7 c2ddecbb f03009f3 4339fa02 af333133 300d0603 2a864886 f70d0101 50500003 82010100 0c8324ef dd3d3cd9 589cfe36 beeb8a80 4b1d1af7 9df3cc53 e829eae3 a1e697c1 589d756c 0e41db4c fad1c12d 50c0eae6 b220255 9d203303 3307c25c 83f8af43 379bea0e 9ac700ee f69c80b3 d97f47a 6d6cd018 7d494aca 99c97198 a2bed877 24f78526 866d8705 404167d1 273aeddcc 481d22dc 0b0b8bcb f4b17bfd 494a98e9 762ae11a 28d76e74 5d38dd1e 22cd6f16 b62b8214 0a945cf2 50ecafce ff62370d ad65d306 4153ed02 14c8b558 28a1ace0 5becb37f 954af003 c8ad26db e6676122 4a99f942 fe1b98e6 42839b8f 8f6724ae 6119b5dd cdb50b26 058ec3a2e 4c87b58b 46cfe218 065ea99e c8819a47 16de0c28 6c2527b9 deb78458 c61f38e4 a4c4cb66 quit
telnet timeout 5
ssh stricthostkeycheck
ssh 10.13.1.0 255.255.255.0 Management
ssh timeout 60
ssh version 2
ssh key-exchange group dh-group1-shal
console timeout 0
no ipv6-vpn-addr-assign aaa
no ipv6-vpn-addr-assign local
t lesbian-detection basic-threat
t threat-detection statistics access-list
no threat-detection statistics tcp-icmp
anyconnect image disk0:/anyconnect-win-4.1.02011-k9.pkg 1 regex "Windows NT"
anyconnect profiles AC3 disk0:/customer3ACprofile.xml
anyconnect enable
cache
disable
error-recovery disable
group-policy DltGrpPolicy attributes
dns-server value 10.13.48.5
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value customer3.com
address-pools value VPN
webvpn
enable internet tis-only
anyconnect image disk0:/anyconnect-win-4.1.02011-k9.pkg 1 regex "Windows NT"
anyconnect profiles AC3 disk0:/customer3ACprofile.xml
anyconnect enable
cache
disable
error-recovery disable
group-policy DltGrpPolicy attributes
dns-server value 10.13.48.5
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value customer3.com
address-pools value VPN
webvpn
anyconnect profiles value AC3 type user
  anyconnect ask none default anyconnect
group-policy vpn internal
group-policy vpn attributes
dns-server value 10.13.48.5
vpn-tunnel-protocol ssl-client
address-pools value VPN
webvpn
  anyconnect profiles value AC3 type user
  anyconnect ask none default anyconnect
dynamic-access-policy-record DfltAccessPolicy
  network-acl allow-all
username admin password <password> encrypted
username vpn-user1 password <password> encrypted
tunnel-group DefaultRASGroup general-attributes
  address-pool VPN
tunnel-group DefaultWEBVPNGroup general-attributes
  address-pool VPN
tunnel-group vpn type remote-access
tunnel-group vpn general-attributes
  address-pool VPN
authorization-server-group LOCAL
default-group-policy vpn
tunnel-group vpn webvpn-attributes
group-alias vpn enable
!
class-map inspection_default
  match default-inspection-traffic
  !
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
policy-map global_policy
class inspection_default
  inspect rtsp
  inspect sunrpc
  inspect xdmcp
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
!
service-policy global_policy
global
prompt hostname context
no call-home reporting anonymous
call-home
http-proxy 64.102.255.40 port 80
profile CiscoTAC-1
  no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly 19
subscribe-to-alert-group configuration periodic monthly 19
subscribe-to-alert-group telemetry periodic daily
profile License

destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
Cryptochecksum: c873b7bdebad06e5d58fab6767d1c2cd
: end
Enterprise Design 2—CSR1000v, ESAv, WSAv, Public AMP, Public Threat Grid

Figure 104  Design 2—CSR1000v, ESAv, WSAv, Public AMP, Public Threat Grid

Design 2

- CSR 1000v
- ESAv
- WSAv
- Public AMP
- Public Threat Grid

MPLS L3 VPN

IP SLA

Gold L3VPN
GE 6 10.13.105.1/24

Gold Internet
GE 7 10.13.8.13/23

Tier 1 Private Network

Tier 2 Private Network

Tier 3 Private Network

Management Network

Management 2 Network

DMZ Network
CSR1000v Configuration

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
platform console auto
!
hostname CU2-CSR1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
enable secret 5 <secret>
enable password <password>
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login line-in local
aaa authorization exec default local
aaa authorization exec line-in if-authenticated
aaa authorization network default local
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip wccp 92 redirect-list WCCP_REDIRECT_IN
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
match access-group name http-ports
match protocol tcp
class-map match-any control-protocols
    match access-group name control-protocols
    match dscp cs6
class-map type inspect match-any web-traffic
    match protocol http
    match protocol https
    match access-group name wsus-ports
    class-map match-all vwaas-control
        match access-group name vwaas-control
class-map match-any ios-pm
    match access-group name ios-pm
class-map match-any call-control
    match dscp cs3
class-map type inspect match-all any-icmp
    match protocol icmp
class-map type inspect match-any private-services
    match protocol ftp
    match protocol sip
    match protocol dns
    match protocol nfs
class-map type inspect match-any smtp-dns
    match protocol smtp
    match protocol dns
class-map type inspect match-any dmz-services
    match protocol dns
class-map type inspect match-any icmp-ssh
    match protocol icmp
    match protocol ssh
class-map type inspect match-any private-vm
    match access-group name tier1-vm
    match access-group name tier2-vm
    match access-group name tier3-vm
class-map type inspect match-all l3vpn-to-esa
    match access-group name exch-to-any
    match protocol smtp
    match access-group name any-to-esa
class-map type inspect match-all internet-to-esa
    match access-group name any-to-esa
    match protocol smtp
class-map type inspect match-all esa-to-exch
    match protocol smtp
    match access-group name esa-to-any
    match access-group name any-to-exch
class-map type inspect match-any wsa-ubiqube-protocols
    match protocol http
    match protocol https
    match protocol ftp
    match protocol icmp
class-map type inspect match-any ubiqube-wsa-protocols
    match protocol http
    match protocol https
    match protocol ftp
    match protocol ssh
    match protocol icmp
    match access-group name wsa-ports
class-map type inspect match-all expanded-dmz-servers
    match class-map private-services
    match access-group name dmz-vm
class-map type inspect match-all private-http-servers
    match class-map private-vm
    match access-group name http-ports
    match protocol tcp
class-map type inspect match-all wsa-to-ubiqube
match access-group name wsa-to-any
match class-map wsa-ubiqube-protocols
match access-group name any-to-ubiqube
class-map type inspect match-all ubiqube-to-wsa
match access-group name ubiqube-to-any
match class-map ubiqube-wsa-protocols
match access-group name any-to-wsa
class-map type inspect match-all dmz-servers
match class-map dmz-services
match access-group name dmz-vm
class-map type inspect match-all private-servers
match class-map private-vm
match class-map private-services
class-map type inspect match-all l3vpn-to-wsa
match access-group name l3vpn-to-any
match access-group name any-to-wsa
match class-map web-traffic
class-map type inspect match-all wsa-to-internet
match access-group name wsa-to-any
match class-map wsa-internet-protocols
class-map type inspect match-all esa-to-internet
match access-group name esa-to-any
match class-map smtp-dns
class-map type inspect match-any web-file-services
match protocol ftp
match protocol dns
match class-map web-traffic
class-map type inspect match-all l3vpn-to-internet
match access-group name l3vpn-to-any
match class-map l3vpn-services
class-map type inspect match-all wsa-to-esa
match access-group name wsa-to-any
match access-group name any-to-esa
match class-map web-file-services
!
policy-map type inspect private-to-internet
class type inspect any-icmp
inspect
class type inspect any-http-servers
inspect log-drop
class class-default
drop log
policy-map internet-egress-qos
class control-protocols
bandwidth 1000
class class-default
fair-queue
random-detect
policy-map type inspect l3vpn-to-internet
class type inspect l3vpn-to-internet
inspect
class type inspect dc-dns-service
inspect
class class-default
drop log
policy-map type inspect internet-to-dmz
class type inspect internet-to-esa
inspect
class class-default
drop log
policy-map type inspect dmz-to-internet
class type inspect esa-to-internet
inspect

class type inspect wsa-to-internet
inspect
class class-default
drop log
policy-map control-plane
class wwaas-control
set dscp cs6
policy-map type inspect private-to-dmz
class type inspect icmp-ssh
inspect
class type inspect dmz-http-servers
inspect log-drop
class type inspect expanded-dmz-servers
inspect log-drop
class class-default
drop log
policy-map type inspect l3vpn-to-private
class type inspect icmp-ssh
inspect
class type inspect private-http-servers
class type inspect private-servers
class class-default
drop log
policy-map type inspect dmz-to-l3vpn
class type inspect esa-to-exch
inspect
class type inspect wsa-to-l3vpn
inspect
class class-default
drop log
policy-map l3vpn-egress-qos
class voip
priority level 1
police 6000000
class control-protocols
bandwidth 1000
class call-control
bandwidth 1000
class class-default
fair-queue
random-detect
policy-map type inspect dmz-to-gold-mgmt
class type inspect wsa-to-ubiqube
inspect
class class-default
drop log
policy-map downlink-egress-qos
class voip
priority level 1 4000
class control-protocols
bandwidth 1000
class call-control
bandwidth 1000
class class-default
fair-queue
random-detect
policy-map type inspect gold-mgmt-to-dmz
class type inspect ubiqube-to-wsa
inspect
class class-default
drop log
policy-map type inspect l3vpn-to-dmz
class type inspect l3vpn-to-wsa
inspect
class type inspect l3vpn-to-esa
  inspect
class class-default
  drop log
!
zone security private
zone security dmz
zone security l3vpn
zone security internet
zone security gold-mgmt
description WSA mgmt
zone-pair security dmz-to-gold-mgmt source dmz destination gold-mgmt
  service-policy type inspect dmz-to-gold-mgmt
zone-pair security dmz-to-internet source dmz destination internet
  service-policy type inspect dmz-to-internet
zone-pair security dmz-to-l3vpn source dmz destination l3vpn
  service-policy type inspect dmz-to-l3vpn
zone-pair security gold-mgmt-to-dmz source gold-mgmt destination dmz
  service-policy type inspect gold-mgmt-to-dmz
zone-pair security internet-to-dmz source internet destination dmz
  service-policy type inspect internet-to-dmz
zone-pair security l3vpn-to-dmz source l3vpn destination dmz
  service-policy type inspect l3vpn-to-dmz
zone-pair security l3vpn-to-internet source l3vpn destination internet
  service-policy type inspect l3vpn-to-internet
zone-pair security l3vpn-to-private source l3vpn destination private
  service-policy type inspect l3vpn-to-private
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1
  ip address 10.13.128.30 255.255.255.240
  ip nat outside
  zone-member security gold-mgmt
  negotiation auto
!
interface GigabitEthernet2
  description gold tier1
  ip address 10.13.101.1 255.255.255.0
  ip nat inside
  ip nbar protocol-discovery
  zone-member security private
  load-interval 30
  negotiation auto
  service-policy output downlink-egress-qos
!
interface GigabitEthernet3
description gold tier2
ip address 10.13.102.1 255.255.255.0
ip nat inside
ip nbar protocol-discovery
zone-member security private
load-interval 30
negotiation auto
service-policy output downlink-egress-qos

interface GigabitEthernet4
description gold tier3
platform ring rx 256
ip address 10.13.103.1 255.255.255.0
ip nat inside
ip nbar protocol-discovery
zone-member security private
load-interval 30
negotiation auto
service-policy output downlink-egress-qos

interface GigabitEthernet5
description gold dmz
platform ring rx 256
ip address 10.13.104.1 255.255.255.0
ip nat inside
ip nbar protocol-discovery
zone-member security dmz
load-interval 30
negotiation auto
service-policy output dmz-egress-qos

interface GigabitEthernet6
description gold l3vpn
platform ring rx 256
ip address 10.13.105.1 255.255.255.0
ip nat inside
ip wccp 92 redirect in
ip nbar protocol-discovery
zone-member security l3vpn
load-interval 30
negotiation auto
service-policy output l3vpn-egress-qos

interface GigabitEthernet7
description gold internet
platform ring rx 256
ip address 10.13.8.13 255.255.254.0
ip nat outside
ip nbar protocol-discovery
zone-member security internet
load-interval 30
negotiation auto
service-policy output internet-egress-qos

interface GigabitEthernet8
description management
platform ring rx 256
ip address 10.13.1.112 255.255.255.0
negotiation auto
router bgp 65513
bgp log-neighbor-changes
neighbor 10.13.9.254 remote-as 109
neighbor 10.13.105.254 remote-as 109

address-family ipv4
redistribute connected route-map inside-interfaces
redistribute static route-map static-routes-to-bgp
neighbor 10.13.9.254 activate
neighbor 10.13.9.254 prefix-list dmz-routes out
neighbor 10.13.9.254 route-map set-nexthop-internet out
neighbor 10.13.105.254 activate
neighbor 10.13.105.254 prefix-list private-routes out
neighbor 10.13.105.254 route-map set-nexthop-l3vpn out
exit-address-family

virtual-service csr_mgmt

ip nat translation finrst-timeout 10
ip nat pool dynamic-nat-pool 10.13.11.103 10.13.11.103 netmask 255.255.255.252
ip nat inside source static 10.13.104.11 10.13.11.21
ip nat inside source static 10.13.104.12 10.13.11.22 extendable
ip nat inside source static 10.13.104.13 10.13.11.23
ip nat inside source static 10.13.104.12 10.13.128.18 extendable
ip nat inside source list dynamic-nat-source pool dynamic-nat-pool overload
ip forward-protocol nd

no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.13.9.254
ip route 10.13.11.11 255.255.255.255 10.13.8.11
ip route 10.13.11.21 255.255.255.255 Null0 tag 1128
ip route 10.13.11.22 255.255.255.255 Null0 tag 1128
ip route 10.13.11.3 255.255.255.255 Null0 tag 1128
ip route 10.13.11.103 255.255.255.255 Null0 tag 1128
ip route 10.13.11.111 255.255.255.255 10.13.104.21 tag 1128
ip route 10.13.11.21 255.255.255.255 10.13.104.21 tag 1128
ip route 10.13.11.22 255.255.255.255 10.13.104.21 tag 1128
ip route 10.13.11.3 255.255.255.255 10.13.104.21 tag 1128
ip route 10.13.11.103 255.255.255.255 10.13.104.21 tag 1128
ip route 64.102.255.40 255.255.255.255 10.13.1.1
ip route 171.70.168.183 255.255.255.255 10.13.1.1
ip route 173.37.145.8 255.255.255.255 10.13.1.1
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 GigabitEthernet1 10.13.1.1

ip access-list extended WCCP_REDIRECT_IN
permit tcp 10.13.32.0 0.0.0.0 255 any eq www
permit tcp 10.13.32.0 0.0.0.0 255 any eq 443
permit tcp 10.13.32.0 0.0.0.0 255 any eq ftp
permit tcp 10.13.32.0 0.0.0.0 255 any eq ftp-data
ip access-list extended any-to-esa
permit ip any host 10.13.104.11
ip access-list extended any-to-exch
permit ip any host 10.13.32.7
ip access-list extended any-to-l3vpn
permit ip any 10.13.32.0 0.0.0.0 255
ip access-list extended any-to-ubiquube
permit ip any host 10.13.128.19
ip access-list extended any-to-wsa
permit ip any host 10.13.104.12
permit ip any host 10.13.128.18
ip access-list extended control-protocols
permit tcp any eq bgp any
permit tcp any any eq bgp
permit udp any any eq 1985
ip access-list extended dc-to-any
permit ip host 10.13.32.5 any
ip access-list extended dmz-vm
permit ip any host 10.13.104.11
permit ip any host 10.13.104.12
permit ip any host 10.13.104.13
permit ip any host 10.13.11.111
ip access-list extended dynamic-nat-source
permit ip host 10.13.101.11 any
permit ip host 10.13.101.12 any
permit ip host 10.13.101.13 any
permit ip host 10.13.102.11 any
permit ip host 10.13.102.12 any
permit ip host 10.13.102.13 any
permit ip host 10.13.103.11 any
permit ip host 10.13.103.12 any
permit ip host 10.13.103.13 any
permit ip 10.13.32.0 0.0.0.255 any
permit ip 10.13.106.0 0.0.0.255 any
ip access-list extended esa-to-any
permit ip host 10.13.104.11 any
ip access-list extended exch-to-any
permit ip host 10.13.32.7 any
ip access-list extended http-ports
permit tcp any any eq www
permit tcp any any eq 8080
permit tcp any any eq 443
ip access-list extended ios-pm
permit tcp any any
ip access-list extended l3vpn-to-any
permit ip 10.13.32.0 0.0.0.255 any
ip access-list extended lv3vpn-to-any
permit ip 10.13.32.0 0.0.0.255 any
ip access-list extended tier1-vm
permit ip any host 10.13.101.11
permit ip any host 10.13.101.12
permit ip any host 10.13.101.13
permit ip any host 10.13.11.111
ip access-list extended tier2-vm
permit ip any host 10.13.102.11
permit ip any host 10.13.102.12
permit ip any host 10.13.102.13
permit ip any host 10.13.112.111
ip access-list extended tier3-vm
permit ip any host 10.13.103.11
permit ip any host 10.13.103.12
permit ip any host 10.13.103.13
permit ip any host 10.13.113.111
ip access-list extended ubiquge-to-any
permit ip host 10.13.128.19 any
ip access-list extended vwaas-control
permit udp any any eq 5787
ip access-list extended web-services
permit tcp any any eq www
permit tcp any any eq 8530
permit tcp any any eq 8531
permit tcp any any eq 443
ip access-list extended wsas-ports
permit tcp any any eq 8443
ip access-list extended wsas-to-any
permit ip host 10.13.104.12 any
ip access-list extended wsas-ports
permit tcp any any eq 8530
permit tcp any any eq 8531
ip prefix-list dmz-routes seq 10 permit 10.13.11.0/24 ge 31
!
ip prefix-list private-routes seq 10 permit 10.13.101.0/24
ip prefix-list private-routes seq 20 permit 10.13.102.0/24
ip prefix-list private-routes seq 30 permit 10.13.103.0/24
ip prefix-list private-routes seq 40 permit 10.13.104.0/24
logging origin-id string ubiqube
logging host 10.13.1.81
!
route-map set-nexthop-internet permit 10
  set ip next-hop 10.13.8.13
!
route-map set-nexthop-l3vpn permit 10
  set ip next-hop 10.13.105.1
!
route-map inside-interfaces permit 10
  match interface GigabitEthernet2 GigabitEthernet3 GigabitEthernet4 GigabitEthernet5
  set metric 1000
!
route-map static-routes-to-bgp permit 10
  match tag 1128
  set metric 1000
!
snmp-server community ubiqube RO
snmp-server host 10.13.1.81 version 2c ubiqube
!
control-plane
  service-policy output control-plane
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
Enterprise Design 3b—ASA, CSR1000v, ESA, WSA, Public AMP, Public Threat Grid

**Figure 105** Design 3b—ASA, CSR1000v, ESA, WSA, Public AMP, Public Threat Grid

Design 3
**ASA Configuration**

ASA Version 9.5(2)204

! terminal width 511
hostname CUS-ASA1
domain-name cisco.com
enable password <password> encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
!
license smart
  feature tier standard
  throughput level 100M
names
ip local pool VPN 10.13.106.101-10.13.106.150 mask 255.255.255.0
!
interface GigabitEthernet0/0
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/1
description gold mgmt-dmz
nameif internal-10.13.128.64
security-level 100
ip address 10.13.128.78 255.255.255.240
!
interface GigabitEthernet0/2
description gold tier1
nameif internal-10.13.101
security-level 75
ip address 10.13.101.1 255.255.255.0
!
interface GigabitEthernet0/3
description gold tier2
nameif internal-10.13.102
security-level 75
ip address 10.13.102.1 255.255.255.0
!
interface GigabitEthernet0/4
description gold tier3
nameif internal-10.13.103
security-level 75
ip address 10.13.103.1 255.255.255.0
!
interface GigabitEthernet0/5
description gold dmz
nameif internal-10.13.104
security-level 50
ip address 10.13.104.1 255.255.255.0
!
interface GigabitEthernet0/6
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/7
description Gold-Internet
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/8
description ASA to CSR
nameif ASAtoCSR
security-level 50
ip address 10.13.192.2 255.255.255.0
policy-route route-map wsa-pbr

interface Management0/0
nameif management
security-level 100
ip address 10.13.1.111 255.255.255.0

ftp mode passive
clock timezone PST -8
dns domain-lookup management
dns server-group DefaultDNS
name-server 171.70.168.183
domain-name cisco.com
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network VPNClients
range 10.13.106.101 10.13.106.150
object network VPNPool
subnet 10.13.106.0 255.255.255.0
description VPNClients
object network cu5-wsa-mgmt
host 10.13.128.66
object network wan-ip
host 10.13.192.2
object network cu5-wsa-internal
host 10.13.104.12
object network cu5-tier1web
host 10.13.101.11
object network cu5-tier2web
host 10.13.102.11
object network cu5-tier3web
host 10.13.103.11
object network cu5-esa-internal
host 10.13.104.11
object network cu5-exch
host 10.13.80.7
object network cu5-dc
host 10.13.80.7
object network ubiquube-nat
host 10.13.128.67
object network lab-internet
subnet 10.13.10.0 255.255.255.0
description Lab Internet
object-group network INSIDE
network-object 10.13.101.0 255.255.255.0
network-object 10.13.102.0 255.255.255.0
network-object 10.13.103.0 255.255.255.0
network-object 10.13.104.0 255.255.255.0
object-group service DM_INLINE_TCP_1 tcp
port-object eq www
port-object eq https
object-group service DM_INLINE_SERVICE_1
  service-object icmp
  service-object tcp destination eq ftp
  service-object tcp destination eq ftp-data
  service-object udp destination eq snmp
object-group network inside-networks
  network-object 10.13.101.0 255.255.255.0
  network-object 10.13.102.0 255.255.255.0
  network-object 10.13.103.0 255.255.255.0
  network-object 10.13.104.0 255.255.255.0
  network-object 10.13.192.0 255.255.255.0
object-group network private-networks
  network-object 10.13.101.0 255.255.255.0
  network-object 10.13.102.0 255.255.255.0
  network-object 10.13.103.0 255.255.255.0
object-group network DM_INLINE_NETWORK_1
  network-object object cu5-tier1web
  network-object object cu5-tier2web
  network-object object cu5-tier3web
object-group service DM_INLINE_TCP_2
  tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_SERVICE_2
  service-object tcp destination eq smtp
  service-object udp destination eq domain
object-group service DM_INLINE_SERVICE_3
  service-object tcp destination eq www
  service-object udp destination eq domain
object-group network DM_INLINE_NETWORK_3
  network-object 10.13.106.0 255.255.255.0
  network-object 10.13.80.0 255.255.255.0
object-group service DM_INLINE_TCP_4
  tcp
  port-object eq www
  port-object eq https
object-group network DM_INLINE_NETWORK_2
  network-object 10.13.106.0 255.255.255.0
  network-object 10.13.80.0 255.255.255.0
access-list allow-all extended permit tcp any any
access-list allow-all extended permit udp any any
access-list allow-all extended permit icmp any any
access-list allow-all extended permit ip object VPNClients any
access-list allow-all extended permit ip 10.13.80.0 255.255.255.0 object VPNPool
access-list wccp-redirect-list extended permit tcp 10.13.80.0 255.255.255.0 10.13.80.0 255.255.255.0 any eq www
access-list wccp-redirect-list extended permit tcp 10.13.80.0 255.255.255.0 10.13.10.0 255.255.255.0 any eq https
access-list wccp-redirect-list extended permit tcp 10.13.80.0 255.255.255.0 10.13.106.0 255.255.255.0 any eq https
access-list wccp-redirect-list extended permit tcp 10.13.80.0 255.255.255.0 10.13.106.0 255.255.255.0 any eq ftp
access-list wccp-redirect-list extended permit tcp 10.13.80.0 255.255.255.0 10.13.10.0 255.255.255.0 any eq ftp-data
access-list wsa-pbr extended permit tcp 10.13.80.0 255.255.255.0 10.13.10.0 255.255.255.0 eq https
access-list wsa-pbr extended permit tcp 10.13.80.0 255.255.255.0 10.13.10.0 255.255.255.0 eq www
access-list wsa-pbr extended permit tcp 10.13.106.0 255.255.255.0 10.13.10.0 255.255.255.0 eq https
access-list wsa-pbr extended permit tcp 10.13.106.0 255.255.255.0 10.13.10.0 255.255.255.0 eq www
access-list dmz extended permit object-group DM_INLINE_SERVICE_1 object cu5-wsa-internal object ubiquube-nat
access-list dmz extended permit tcp object cu5-wsa-internal object cu5-exch eq smtp
access-list dmz extended permit object-group DM_INLINE_SERVICE_3 object cu5-wsa-internal any
access-list dmz extended permit object-group DM_INLINE_SERVICE_2 object cu5-esa-internal any
access-list asa-to-csr extended permit tcp any object cu5-wsa-internal object-group DM_INLINE_TCP_1
access-list asa-to-csr extended permit tcp object cu5-exch object cu5-esa-internal eq smtp
access-list asa-to-csr extended permit tcp object-group DM_INLINE_NETWORK_3 object-group DM_INLINE_NETWORK_1 object-group DM_INLINE_TCP_2
access-list asa-to-csr extended permit tcp object-group DM_INLINE_NETWORK_2 any object-group DM_INLINE_TCP_4
access-list asa-to-csr extended deny tcp 10.13.80.0 255.255.255.0 object cu5-esa-internal eq smtp
access-list asa-to-csr extended permit tcp any object cu5-esa-internal eq smtp
access-list sslvpn extended permit tcp object VPNClients object-group inside-networks eq https
access-list sslvpn extended permit icmp object VPNClients object-group inside-networks
access-list internal-10.13.102_access_in extended deny ip any any
access-list internal-10.13.103_access_in extended deny ip any any
access-list internal-10.13.101_access_in extended deny ip any any
pager lines 24
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging history informational
logging asdm informational
logging facility 21
logging device-id string SPA165
logging host management 10.13.1.81
mtu internal-10.13.128.64 1500
mtu internal-10.13.101 1500
mtu internal-10.13.102 1500
mtu internal-10.13.103 1500
mtu internal-10.13.104 1500
mtu ASAtoCSR 1500
mtu management 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (ASAtoCSR,internal-10.13.104) source static VPNPool VPNPool
nat (ASAtoCSR,internal-10.13.103) source static VPNPool VPNPool
nat (ASAtoCSR,internal-10.13.102) source static VPNPool VPNPool
nat (ASAtoCSR,internal-10.13.101) source static VPNPool VPNPool
nat (internal-10.13.104,internal-10.13.128.64) source static cu5-wsa-internal cu5-wsa-mgmt
access-group internal-10.13.101_access_in in interface internal-10.13.101
access-group internal-10.13.102_access_in in interface internal-10.13.102
access-group internal-10.13.103_access_in in interface internal-10.13.103
access-group dmz in interface internal-10.13.104
access-group asa-to-csr in interface ASAtoCSR
! 
prefix-list private-routes seq 10 permit 10.13.101.0/24
prefix-list private-routes seq 20 permit 10.13.102.0/24
prefix-list private-routes seq 30 permit 10.13.103.0/24
prefix-list private-routes seq 40 permit 10.13.104.0/24
! 
route-map inside-interfaces permit 10
match interface internal-10.13.101 internal-10.13.102 internal-10.13.103 internal-10.13.104
set metric 1000

! route-map wsa-pbr permit 10
match ip address wsa-pbr
set ip next-hop 10.13.104.12

! router ospf 100
network 10.13.101.0 255.255.255.0 area 0
network 10.13.102.0 255.255.255.0 area 0
network 10.13.103.0 255.255.255.0 area 0
network 10.13.104.0 255.255.255.0 area 0
network 10.13.192.0 255.255.255.0 area 0
log-adj-changes
redistribute static subnets

! route ASAtoCSR 0.0.0.0 0.0.0.0 10.13.192.1 1
route management 64.102.255.40 255.255.255.0 10.13.1.1 1
route management 72.163.4.38 255.255.255.0 10.13.1.1 1
route management 171.70.168.183 255.255.255.0 10.13.1.1 1
route management 173.37.145.8 255.255.255.0 10.13.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.13.1.0 255.255.255.0 management
snmp-server host management 10.13.1.81 poll community ubiqube
no snmp-server location
no snmp-server contact
snmp-server community ubiqube
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint _SmartCallHome_ServerCA
no validation-usage
crl configure
crypto ca trustpool policy
crypto ca_certificate chain _SmartCallHome_ServerCA
certificate ca 6ecc7aa5a7032009b8cebcf4e952d491
308205ec 308204d4 a0030201 02020106 cc7aa5a7 032009b8 cebcf4e9 52d49130
0d06092a 864886f7 0d010105 05003081 ca110b30 09060355 04061302 55533117
30150603 55040a13 0e566572 69536967 6e2c2049 6e6132e1 1f301d06 0355040b
13156665 72695369 676e2e05 72757374 204e6574 776f726b 313a3038 06035504
0b133128 63292032 30303620 56657269 5369676e 2c203038 632e020d 20466f72
20617574 686f7269 7a6e6420 75736520 436c6173 73203320 5075626c 20434120
496e6173 73203320 5075626c 20434120 20547774 20472065 20472065 20472065
6572696c 6573696e 20313232 31333333 31343536 31363738 31373839 31393a30
30090003 05504063 17301506 0355040a 130e6565 72695369 676e2e02 54777473
4777ff72 6b313b30 39060355 040b1332 5465726d 73206f6e 20757365 20617440
68747470 733a2f2f 7777772e 76657269 7369676e 2e636f6d 2f727061 2f628539
3130312f 302d0603 55504033 26566572 69536967 6e2e043c 61773732 33205365
63757265 20536572 76657220 4341202d 20473330 20812300 2000092a 864886f7
0d010101 05000382 010f0003 202010a2 2020100b 1b87841f 0c0c45f5 bcab2597
a7ada23e 9caab6c1 39b8bca c2ac56c6 e5bb658e 444f4dce 6f6f094a d4af4e10
9c688b2e 957b899b 13ca2e34 34df35b f3497b62 83488174 d188786c 0253f9bc
group-policy vpn internal
group-policy vpn attributes
dns-server value 10.13.80.5
vpn-tunnel-protocol ssl-client
address-pools value VPN
webvpn
  anyconnect profiles value AC2 type user
  anyconnect ask none default anyconnect
dynamic-access-policy-record DfltAccessPolicy
  network-acl allow-all
username admin password <password> encrypted
username vpn-user1 password <password> encrypted
tunnel-group DefaultRAGroup general-attributes
  address-pool VPN
tunnel-group DefaultWEBVPNGroup general-attributes
  address-pool VPN
tunnel-group vpn type remote-access
tunnel-group vpn general-attributes
  address-pool VPN
  authorization-server-group LOCAL
default-group-policy vpn
tunnel-group vpn webvpn-attributes
  group-alias vpn enable
! class-map inspection_default
  match default-inspection-traffic
! policy-map type inspect dns preset_dns_map	parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
  inspect ip-options
  inspect netbios
  inspect rtsp
  inspect sunrpc
  inspect tftp
  inspect xdmcp
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect reh
  inspect esmtp
  inspect sqlnet
  inspect sip
  inspect skinny
policy-map type inspect dns migrated_dns_map_1	parameters
  message-length maximum client auto
  message-length maximum 512
!

service-policy global_policy global
prompt hostname context
service call-home
call-home reporting anonymous prompt 1
call-home
http-proxy 64.102.255.40 port 80
profile CiscoTAC-1
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly 20
subscribe-to-alert-group configuration periodic monthly 20
subscribe-to-alert-group telemetry periodic daily
profile license
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
Cryptochecksum:8fe9dde7f90980aea4aaafcd0ed733979
: end

CSR1000V Configuration

version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
platform console auto
!
hostname CU5-CSR1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 <secret>
enable password <password>
!

aaa new-model
!
!
aaa authentication login line-in local
aaa authorization exec default local
aaa authorization exec line-in if-authenticated
!
!
!
!
!
!
!
!
!
!

aaa session-id common

clock timezone PST -8 0
call-home
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip name-server 171.70.168.183

ip domain name customer5.com

subscribe templating

parameter-map type inspect-global
log dropped-packets

parameter-map type inspect log-drop
log dropped-packets

multilink bundle-name authenticated

crypto pki trustpoint TP-self-signed-515365235
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-515365235
revocation-check none
rsakeypair TP-self-signed-515365235

! crypto pki trustpoint SLA-TrustPoint
enrollment terminal
revocation-check crl

! crypto pki certificate chain TP-self-signed-515365235
crypto pki certificate chain SLA-TrustPoint

Certificate ca 01
30820321 30820209 A030201 02020101 300D0609 2A864886 F70D0101 0B050030
32330E30 0C060355 040A1305 43697363 6F204C69 63656E73 696E6720 526F6F74 20434130 82012230 0D06092A 864886F7 0D010105 00003820
82010A02 82010100 A6C8D696 131E05F7 145EA72C 2CD686E6 17222EA1 F1E8F64D CB4C798 212AA14 7C655D87 9471380D 8711441E 1A9E6188 8A38E520 1C394D78 462E9239 C659F715 B980A59 5B85CBD0 C6F8EA3 700A89F7 D8F256EE 4A44B80D DB86D1C9 6081FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC 7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD21CF 58BD7188 68EB9491 20F320B7 94BE7D7 AE3BCCB4 F01684C7 4BC8E00F 539BA42B 42C688B7 C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B 82850FC4 5D5DF8B8 F87D9191 C55F9D76 61F9A4CD 3D992327 A8BB03BD 4E67D069 7CBAD7F8 3DF5F4368 95135E44 DFC7C6CF 04D77FDD 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201 06300F06 03551D13 0101F004 05300301 01FF010D 0603551D 0E041604 1449DC85 4B3D31E5 B3E6A173 60A63333 3D3B4C73 E300D06 092A8648 86F70001 01080500 03820101 00507F24 D3932A66 86025DF9 EB38A5EC 6D4DF6B0 49631C78 240DA905 604EDCDE FF4FED2B 77FC460E CD63F6B7 DD4688E 3A5671A9 9093DB1 6C9E3D8B D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD988B46 5575B146 8DFC66A8
Appendix D—HSS Enterprise Designs Tested

467A3DF4 4D565700 6ADF0F0D 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5F0D3A06 B92AFE7F 494E8A9E 07BB8737 F3A58BBE 1A48A229 C37C1E69 39F08678
80D9C162 D6BACECA EEB77CF9 8428787B 35202C0D 0B4C501F 230E3AFB
248616A9 4093E049 4D10AB75 27E86F73 912E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28

quit

license udi pid CSR1000V sn 9FWIKTCC22I
license boot level ax
license smart enable

object-group network inside-networks
10.13.101.0 255.255.255.0
10.13.102.0 255.255.255.0
10.13.103.0 255.255.255.0
10.13.104.0 255.255.255.0
10.13.105.0 255.255.255.0
10.13.106.0 255.255.255.0

spanning-tree extend system-id
username admin password 0 IsSecurity!
redundancy
cdp run

class-map match-any voip
match dscp ef
class-map type inspect match-all dc-dns-service
match access-group name dc-to-any
match protocol dns
class-map type inspect match-all internet-to-sslvpn
match protocol https
match access-group name any-to-sslvpn
class-map match-any control-protocols
match access-group name control-protocols
match dscp cs6
class-map type inspect match-any web-traffic
match protocol http
match protocol https
match access-group name wsus-ports
match protocol dns
class-map match-all vwaas-control
match access-group name vwaas-control
class-map match-any call-control
match dscp cs3
class-map type inspect match-any smtp-dns
match protocol smtp
class-map type inspect match-all l3vpn-to-esa
match access-group name exch-to-any
match protocol smtp
class-map type inspect match-all esa-to-l3vpn
match access-group name any-to-exch
match protocol smtp
class-map type inspect match-all internet-to-esa
match access-group name any-to-esa
class-map type inspect match-any web-file-services
match protocol ftp
match access-group name any-to-esa
class-map type inspect match-all l3vpn-to-internet
match protocol smtp
match access-group name any-to-internet
class-map type inspect match-all l3vpn-to-private
match access-group name any-to-private
class-map type inspect match-all l3vpn-to-wsa
match access-group name any-to-wsa
!
 policy-map type inspect asa-to-l3vpn
 class type inspect wsa-to-l3vpn
 inspect
class type inspect esa-to-l3vpn
 inspect
class type inspect sslvpn-to-l3vpn
 inspect
class class-default
drop log
policy-map internet-egress-qos
class control-protocols
 bandwidth 1000
class class-default
 fair-queue
 random-detect
policy-map type inspect l3vpn-to-internet
class type inspect l3vpn-to-internet
 inspect
class type inspect dc-dns-service
inspect
class class-default
drop log
policy-map control-plane
class wvaas-control
set dscp cs6
policy-map type inspect CSRtoASA-to-internet
class type inspect wsa-to-internet
inspect
class type inspect esa-to-internet
inspect
class class-default
drop log
policy-map type inspect l3vpn-to-asa
class type inspect l3vpn-to-wsa
inspect
class type inspect l3vpn-to-esa
inspect
class type inspect l3vpn-to-private
inspect
class class-default
drop log
policy-map type inspect Internet-to-CSRtoASA
class type inspect Internet-to-wsa
inspect
class type inspect Internet-to-esa
inspect
class type inspect Internet-to-ssl vpn
inspect
class class-default
drop log
policy-map l3vpn-egress-qos
class voip
  priority level 1
  police 6000000
class control-protocols
  bandwidth 1000
class call-control
  bandwidth 1000
class class-default
  fair-queue
  random-detect
policy-map downlink-egress-qos
class voip
  priority level 1 4000
class control-protocols
  bandwidth 1000
class call-control
  bandwidth 1000
class class-default
  fair-queue
  random-detect
!
zone security l3vpn
zone security internet
zone security CSRtoASA
zone-pair security CSRtoASA-to-internet source CSRtoASA destination internet
service-policy type inspect CSRtoASA-to-internet
zone-pair security CSRtoASA-to-l3vpn source CSRtoASA destination l3vpn
service-policy type inspect asa-to-l3vpn
zone-pair security Internet-to-CSRtoASA source internet destination CSRtoASA
service-policy type inspect Internet-to-CSRtoASA
zone-pair security l3vpn-to-CSRtoASA source l3vpn destination CSRtoASA
service-policy type inspect l3vpn-to-asa
zone-pair security l3vpn-to-internet source l3vpn destination internet
service-policy type inspect l3vpn-to-internet
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet1
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet2
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet3
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet4
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet5
  no ip address
  shutdown
  negotiation auto
!
interface GigabitEthernet6
  description gold l3vpn
  platform ring rx 256
  ip address 10.13.105.1 255.255.255.0
  ip nat inside
  zone-member security l3vpn
  ip policy route-map wsa-pbr
  negotiation auto
  service-policy output l3vpn-egress-qos
!
interface GigabitEthernet7
  description gold internet
  platform ring rx 256
  ip address 10.13.8.19 255.255.254.0
  ip nat outside
zone-member security internet
negotiation auto
service-policy output internet-egress-qos
interface GigabitEthernet8
description CSRtoASA
platform ring rx 256
ip address 10.13.192.1 255.255.255.0
ip nat inside
zone-member security CSRtoASA
negotiation auto
interface GigabitEthernet9
description Management
platform ring rx 256
ip address 10.13.1.22 255.255.255.0
negotiation auto
router ospf 100
redistribute static subnets route-map static2ospf
redistribute bgp 65513 subnets
network 10.13.192.0 0.0.0.255 area 0
router bgp 65513
bgp log-neighbor-changes
neighbor 10.13.9.254 remote-as 109
neighbor 10.13.105.254 remote-as 109
address-family ipv4
redistribute static
neighbor 10.13.9.254 activate
neighbor 10.13.9.254 prefix-list public-routes out
neighbor 10.13.105.254 activate
neighbor 10.13.105.254 prefix-list private-routes out
exit-address-family
virtual-service csr_mgmt
ip nat translation finrst-timeout 10
ip nat inside source static 10.13.104.11 10.13.11.51
ip nat inside source static 10.13.104.12 10.13.11.52
ip nat inside source static 10.13.192.2 10.13.11.53
ip nat inside source list INSIDE interface GigabitEthernet7 overload
ip forward-protocol nd
no ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.13.9.254
ip route 10.13.11.51 255.255.255.255 Null0
ip route 10.13.11.52 255.255.255.255 Null0
ip route 10.13.11.53 255.255.255.255 Null0
ip route 64.102.255.40 255.255.255.255 10.13.1.1
ip route 171.70.168.183 255.255.255.255 10.13.1.1
ip route 173.37.145.8 255.255.255.255 10.13.1.1
ip access-list extended CAPTURE
permit tcp any any
ip access-list extended INSIDE
permit ip 10.13.192.0 0.0.0.255 any
permit ip 10.13.101.0 0.0.0.255 any
permit ip 10.13.102.0 0.0.0.255 any
permit ip 10.13.103.0 0.0.0.255 any
permit ip 10.13.104.0 0.0.0.255 any
permit ip 10.13.105.0 0.0.0.255 any
permit ip 10.13.106.0 0.0.0.255 any
permit ip 10.13.80.0 0.0.0.255 any
ip access-list extended allow-all
permit ip any any log
ip access-list extended any-to-esa
permit ip any host 10.13.104.11
ip access-list extended any-to-exch
permit ip any host 10.13.80.7
ip access-list extended any-to-l3vpn
permit ip any 10.13.80.0 0.0.0.255
ip access-list extended any-to-private
permit ip any host 10.13.101.10
permit ip any host 10.13.102.10
permit ip any host 10.13.103.10
permit ip any host 10.13.101.11
permit ip any host 10.13.102.11
permit ip any host 10.13.103.11
ip access-list extended any-to-sslvpn
permit ip any host 10.13.192.2
ip access-list extended any-to-vpn
permit ip any host 10.13.192.2
ip access-list extended any-to-wsa
permit ip any host 10.13.104.12
deny ip any object-group inside-networks
permit ip any any
ip access-list extended capture-l3vpn
permit ip any any
ip access-list extended dc-to-any
permit ip host 10.13.80.5 any
ip access-list extended esa-to-any
permit ip host 10.13.104.11 any
ip access-list extended exch-to-any
permit ip host 10.13.80.7 any
ip access-list extended inside-networks
permit ip any any
ip access-list extended l3vpn-to-any
permit ip 10.13.80.0 0.0.0.255 any
ip access-list extended lv3vpn-to-any
permit ip 10.13.80.0 0.0.0.255 any
ip access-list extended sslvpn
permit ip any host 10.13.192.2
ip access-list extended sslvpn-to-any
permit ip 10.13.106.0 0.0.0.255 any
ip access-list extended wsa-pbr
permit tcp 10.13.80.0 0.0.0.255 10.13.10.0 0.0.0.255 eq www
permit tcp 10.13.80.0 0.0.0.255 10.13.10.0 0.0.0.255 eq 443
ip access-list extended wsa-to-any
permit ip host 10.13.104.12 any
ip access-list extended wsus-ports
permit tcp any any eq 8530
permit tcp any any eq 8531
!
ip prefix-list private-routes seq 10 permit 10.13.106.0/24
!
ip prefix-list public-routes seq 10 permit 10.13.11.51/32
ip prefix-list public-routes seq 20 permit 10.13.11.52/32
ip prefix-list public-routes seq 30 permit 10.13.11.53/32
logging origin-id string SPA129
logging host 10.13.1.81
access-list 1 permit 0.0.0.0
access-list 101 permit tcp any host 10.13.104.12
!
route-map static2ospf permit 10
match ip address 1
!
route-map wsa-pbr permit 10
match ip address wsa-pbr
set ip next-hop 10.13.192.2
!

snmp-server community ubiqube RO
snmp-server host 10.13.1.81 version 2c ubiqube
!
!
!

control-plane
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
Enterprise Design 4—ASAv, ESAv, WSAv, Private AMP Shared and Private Threat Grid

Figure 106  Design 4—ASAv, ESAv, WSAv, Private AMP Shared and Private Threat Grid

HSS Enterprise Design #4

ASAv Configuration

Refer to Enterprise Design 1 for the ASAv configuration.
Enterprise Design 5—ASAv, ESAv, WSAv, Private AMP Dedicated and Private Threat Grid

HSS Enterprise Design #5

ASAv Configuration

Refer to Enterprise Design 1b for the ASAv configuration.
Appendix E—HSS SMB Designs Tested

SMB Design 1b—ASA v, Shared ESA v, Shared WSA v, Private AMP Shared and Private AMP Threat Grid

Figure 108 SMB Design 1b—ASA v, Shared ESA v, Shared WSA v, Private AMP Shared and Private Threat Grid

HSS SMB Design #1
ASA v Configuration

- Saved

- Serial Number: 9ACAPB69A9W
- Hardware:  ASA v, 1024 MB RAM, CPU Xeon ES series 2294 MHz
- Written by enable_15 at 16:42:54.519 PDT Thu Oct 6 2016

ASA Version 9.6(2)

hostname SPB-ASA v5-1
domain-name cisco.com
enable password eJUMu/fWRcXX9aU encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain

license smart
feature tier standard
throughput level 100M
names
dns-guard
ip local pool CU1_VPN_POOL 10.13.201.101-10.13.201.150 mask 255.255.255.0
ip local pool CU3_VPN_POOL 10.13.203.101-10.13.203.150 mask 255.255.255.0
ip local pool CU4_VPN_POOL 10.13.204.101-10.13.204.150 mask 255.255.255.0
ip local pool CU5_VPN_POOL 10.13.205.101-10.13.205.150 mask 255.255.255.0
ip local pool CU6_VPN_POOL 10.13.206.101-10.13.206.150 mask 255.255.255.0

interface GigabitEthernet0/0
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/1
description silver MANAGEMENT 2
nameif INTERNAL_10.13.128.96
security-level 100
ip address 10.13.128.110 255.255.255.240

interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address

interface GigabitEthernet0/5
description DMZ
nameif INTERNAL_10.13.104
security-level 25
ip address 10.13.104.1 255.255.255.0

interface GigabitEthernet0/6
no nameif
no security-level
no ip address

interface GigabitEthernet0/6.301
description CU1 L3VPN
vlan 301
nameif CU1_L3VPN
security-level 50
ip address 10.13.105.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/6.302
description CU2 L3VPN
vlan 302
nameif CU2_L3VPN
security-level 50
ip address 10.13.106.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/6.303
description CU3 L3VPN
vlan 303
nameif CU3_L3VPN
security-level 50
ip address 10.13.107.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/6.304
description CU4 L3VPN
vlan 304
nameif CU4_L3VPN
security-level 50
ip address 10.13.108.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/6.305
description CU5 L3VPN
vlan 305
nameif CU5_L3VPN
security-level 50
ip address 10.13.109.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/6.306
description CU6 L3VPN
vlan 306
nameif CU6_L3VPN
security-level 50
ip address 10.13.110.1 255.255.255.0
policy-route route-map WSA_PBR

interface GigabitEthernet0/7
description INTERNET
nameif INTERNET
  security-level 0
  ip address 10.13.8.27 255.255.254.0

interface GigabitEthernet0/8
  shutdown
  no nameif
  no security-level
  no ip address

interface Management0/0
  nameif MANAGEMENT
  security-level 100
  ip address 10.13.1.135 255.255.255.0

ftp mode passive

clock timezone PST -8

clock summer-time PDT recurring

dns domain-lookup MANAGEMENT

dns server-group CU1_DNS
  name-server 10.13.16.5
  domain-name customer1.com

dns server-group CU2_DNS
  name-server 10.13.32.5
  domain-name customer2.com

dns server-group CU3_DNS
  name-server 10.13.48.5
  domain-name customer3.com

dns server-group CU4_DNS
  name-server 10.13.64.5
  domain-name customer4.com

dns server-group CU5_DNS
  name-server 10.13.80.5
  domain-name customer5.com

dns server-group CU6_DNS
  name-server 10.13.96.5
  domain-name customer6.com

dns server-group DefaultDNS
  name-server 171.70.168.183
  domain-name cisco.com

object network SPB_ESA1_INT
  host 10.13.104.11

object network SPB_ESA1_EXT
  host 10.13.11.71

object network SPB_WSA1_MGMT2
  host 10.13.128.98

object network CU1_EXCH1
  host 10.13.16.7

object network CU1_DC1
  host 10.13.16.5

object network CU2_EXCH1
  host 10.13.32.7

object network CU2_DC1
  host 10.13.32.5

object network CU3_EXCH1
  host 10.13.48.7

object network CU3_DC1
  host 10.13.48.5

object network CU4_EXCH1
  host 10.13.64.7

object network CU4_DC1
  host 10.13.64.5
object network CU5_EXCH1
  host 10.13.80.7
object network CU5_DC1
  host 10.13.80.5
object network CU6_EXCH1
  host 10.13.96.7
object network CU6_DC1
  host 10.13.96.5
object network UBIQUBE_MGMT2
  host 10.13.128.99
object network CU1_VPN_CUSTOMERS
  object network CU1_VPN_POOL
    subnet 10.13.201.0 255.255.255.0
  object network CU1_VPN_CUSTOMERS
  range 10.13.201.101 10.13.201.150
object network CU1_VPN_POOL
  subnet 10.13.202.0 255.255.255.0
object network CU2_VPN_CUSTOMERS
  object network CU2_VPN_POOL
  object network CU2_VPN_CUSTOMERS
object network CU2_VPN_POOL
  subnet 10.13.203.0 255.255.255.0
object network CU3_VPN_CUSTOMERS
  object network CU3_VPN_POOL
    subnet 10.13.203.101 10.13.203.150
  object network CU3_VPN_CUSTOMERS
  range 10.13.203.101 10.13.203.150
object network CU3_VPN_POOL
  subnet 10.13.204.0 255.255.255.0
object network CU4_VPN_CUSTOMERS
  object network CU4_VPN_POOL
    subnet 10.13.205.0 255.255.255.0
  object network CU4_VPN_CUSTOMERS
  range 10.13.204.101 10.13.204.150
object network CU4_VPN_POOL
  subnet 10.13.206.0 255.255.255.0
object network CU5_VPN_CUSTOMERS
  object network CU5_VPN_POOL
    subnet 10.13.205.101 10.13.205.150
  object network CU5_VPN_CUSTOMERS
  range 10.13.205.101 10.13.205.150
object network CU5_VPN_POOL
  subnet 10.13.206.0 255.255.255.0
object network CU6_VPN_CUSTOMERS
  object network CU6_VPN_POOL
    subnet 10.13.206.101 10.13.206.150
  object network CU6_VPN_CUSTOMERS
  range 10.13.206.101 10.13.206.150
object network CU6_VPN_POOL
  subnet 10.13.206.0 255.255.255.0
object service WSUS_SVC
  service tcp destination range 8530 8531
object-group network ALL_EXCH
  network-object object CU1_EXCH1
  network-object object CU2_EXCH1
  network-object object CU3_EXCH1
  network-object object CU4_EXCH1
  network-object object CU5_EXCH1
  network-object object CU6_EXCH1
object-group network ALL_DC
  network-object object CU1_DC1
  network-object object CU2_DC1
  network-object object CU3_DC1
  network-object object CU4_DC1
  network-object object CU5_DC1
  network-object object CU6_DC1
Appendix E—HSS SMB Designs Tested

object-group network ALL_L3VPN
    network-object object CU1_L3VPN_NET
    network-object object CU2_L3VPN_NET
    network-object object CU3_L3VPN_NET
    network-object object CU4_L3VPN_NET
    network-object object CU5_L3VPN_NET
    network-object object CU6_L3VPN_NET
object-group network ALL_L3VPN_NET
    network-object object CU1_L3VPN_NET
    network-object object CU2_L3VPN_NET
    network-object object CU3_L3VPN_NET
    network-object object CU4_L3VPN_NET
    network-object object CU5_L3VPN_NET
    network-object object CU6_L3VPN_NET

object-group service WEB_SVC
    service-object tcp destination eq www
    service-object tcp destination eq https
    service-object tcp destination eq ftp
    service-object tcp destination eq domain
    service-object icmp
    object-group service UBIQUE_SVC
        service-object icmp
        service-object tcp destination eq https
        service-object tcp destination eq www
        service-object tcp destination eq ftp
        service-object tcp destination eq ftp-data
        service-object tcp destination eq ssh
        service-object udp destination eq snmp
        service-object icmp echo
        service-object icmp echo-reply
    object-group service EXCH_SVC
        service-object tcp destination eq www
        service-object tcp destination eq https
        service-object tcp destination eq imap4
        service-object icmp
    object-group service DC_SVC
        service-object tcp destination eq ldap
        service-object tcp-udp destination eq domain
        service-object udp destination eq 389
        service-object tcp destination eq 88
        service-object tcp destination eq 445
        service-object icmp
    access-list WSA_PBR extended deny tcp any object SPB_WSA1_INT eq www
    access-list WSA_PBR extended deny tcp any object SPB_WSA1_INT eq https
    access-list WSA_PBR extended permit tcp object-group ALL_L3VPN_NET any eq https
    access-list WSA_PBR extended permit tcp object-group ALL_L3VPN_NET any eq www
    access-list CU1_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object CU1_VPN_CLIENTS object CU1_EXCH1
    access-list CU1_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU1_VPN_CLIENTS object CU1_DC1
    access-list CU1_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object CU1_VPN_CLIENTS object SPB_WSA1_INT
    access-list CU2_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object CU2_VPN_CLIENTS object CU2_EXCH1
    access-list CU2_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU2_VPN_CLIENTS object CU2_DC1
    access-list CU2_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object CU2_VPN_CLIENTS object SPB_WSA1_INT
    access-list AnyConnect_Client_Local_Print extended deny ip any4 any4
    access-list AnyConnect_Client_Local_Print extended permit tcp any4 any4 eq lpd
    access-list AnyConnect_Client_Local_Print remark IPP: Internet Printing Protocol
    access-list AnyConnect_Client_Local_Print extended permit tcp any4 any4 eq 631
    access-list AnyConnect_Client_Local_Print remark Windows' printing port
Appendix E—HSS SMB Designs Tested

access-list AnyConnect_Client_Local_Print extended permit tcp any4 any4 eq 9100
access-list AnyConnect_Client_Local_Print remark mDNS: multicast DNS protocol
access-list AnyConnect_Client_Local_Print extended permit udp any4 host 224.0.0.251 eq 5353
access-list AnyConnect_Client_Local_Print remark LLMNR: Link Local Multicast Name Resolution protocol
access-list AnyConnect_Client_Local_Print extended permit udp any4 host 224.0.0.252 eq 5355
access-list AnyConnect_Client_Local_Print remark TCP/NetBIOS protocol
access-list AnyConnect_Client_Local_Print extended permit tcp any4 any4 eq 137
access-list DMZ_ACL extended permit tcp object SPB_ESA1_INT object-group ALL_EXCH eq smtp
access-list DMZ_ACL extended deny tcp object SPB_ESA1_INT object-group ALL_L3VPN_NET eq smtp
access-list DMZ_ACL extended permit tcp object SPB_ESA1_INT any eq smtp
access-list DMZ_ACL extended permit object-group DC_SVC object SPB_ESA1_INT object-group ALL_DC
access-list DMZ_ACL extended permit udp object SPB_ESA1_INT any eq domain
access-list DMZ_ACL extended permit icmp object SPB_ESA1_INT any
access-list DMZ_ACL extended permit object-group DC_SVC object SPB_WSA1_INT object-group ALL_DC
access-list DMZ_ACL extended deny tcp object SPB_WSA1_INT object-group ALL_L3VPN_NET
access-list DMZ_ACL extended permit tcp object SPB_WSA1_INT any eq domain
access-list INTERNET_ACL extended permit tcp any object SPB_WSA1_EXT eq smtp
access-list CU1_L3VPN_ACL extended deny ip object CU1_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU1_L3VPN_ACL extended permit tcp object CU1_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU1_L3VPN_ACL extended permit object-group WEB_SVC object CU1_L3VPN_NET any
access-list CU1_L3VPN_ACL extended permit icmp any any
access-list CU1_L3VPN_ACL extended permit udp object CU1_DC1 any eq domain
access-list CU2_L3VPN_ACL extended deny ip object CU2_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU2_L3VPN_ACL extended permit tcp object CU2_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU2_L3VPN_ACL extended permit object-group WEB_SVC object CU2_L3VPN_NET any
access-list CU2_L3VPN_ACL extended permit icmp any any
access-list CU2_L3VPN_ACL extended permit udp object CU2_DC1 any eq domain
access-list CU3_L3VPN_ACL extended deny ip object CU3_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU3_L3VPN_ACL extended permit tcp object CU3_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU3_L3VPN_ACL extended permit object-group WEB_SVC object CU3_L3VPN_NET any
access-list CU3_L3VPN_ACL extended permit icmp any any
access-list CU3_L3VPN_ACL extended permit udp object CU3_DC1 any eq domain
access-list CU4_L3VPN_ACL extended deny ip object CU4_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU4_L3VPN_ACL extended permit tcp object CU4_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU4_L3VPN_ACL extended permit object-group WEB_SVC object CU4_L3VPN_NET any
access-list CU4_L3VPN_ACL extended permit icmp any any
access-list CU4_L3VPN_ACL extended permit udp object CU4_DC1 any eq domain
access-list CU5_L3VPN_ACL extended deny ip object CU5_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU5_L3VPN_ACL extended permit tcp object CU5_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU5_L3VPN_ACL extended permit object-group WEB_SVC object CU5_L3VPN_NET any
access-list CU5_L3VPN_ACL extended permit icmp any any
access-list CU5_L3VPN_ACL extended permit udp object CU5_DC1 any eq domain
access-list CU6_L3VPN_ACL extended deny ip object CU6_L3VPN_NET object-group ALL_L3VPN_NET
access-list CU6_L3VPN_ACL extended permit tcp object CU6_EXCH1 object SPB_ESA1_INT eq smtp
access-list CU6_L3VPN_ACL extended permit udp object CU6_DC1 any eq domain
access-list CU6_L3VPN_ACL extended permit object-group WEB_SVC object CU6_L3VPN_NET any
access-list CU6_L3VPN_ACL extended permit icmp any any
access-list CU6_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object
CU6_VPN_CLIENTS object CU6_EXCH1
access-list CU6_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU6_VPN_CLIENTS object CU6_DC1
access-list CU6_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object
CU6_VPN_CLIENTS object SPB_WSA1_INT
access-list CU3_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object
CU3_VPN_CLIENTS object CU3_EXCH1
access-list CU3_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU3_VPN_CLIENTS object CU3_DC1
access-list CU3_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object
CU3_VPN_CLIENTS object SPB_WSA1_INT
access-list CU4_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object
CU4_VPN_CLIENTS object CU4_EXCH1
access-list CU4_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU4_VPN_CLIENTS object CU4_DC1
access-list CU4_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object
CU4_VPN_CLIENTS object SPB_WSA1_INT
access-list CU5_VPN_CLIENTS_ACL extended permit object-group EXCH_SVC object
CU5_VPN_CLIENTS object CU5_EXCH1
access-list CU5_VPN_CLIENTS_ACL extended permit object-group DC_SVC object CU5_VPN_CLIENTS object CU5_DC1
access-list CU5_VPN_CLIENTS_ACL extended permit object-group WEB_SVC object
CU5_VPN_CLIENTS object SPB_WSA1_INT
pager lines 23
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging history informational
logging asdm informational
logging facility 21
logging device-id string SPB189
logging host MANAGEMENT 10.13.1.81
mtu INTERNAL_10.13.128.96 1500
mtu INTERNAL_10.13.104 1500
mtu CU1_L3VPN 1500
mtu CU2_L3VPN 1500
mtu CU3_L3VPN 1500
mtu CU4_L3VPN 1500
mtu CU5_L3VPN 1500
mtu CU6_L3VPN 1500
mtu INTERNET 1500
mtu MANAGEMENT 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
nat (INTERNAL_10.13.104,INTERNET) source static SPB_WSA1_INT SPB_WSA1_EXT
nat (CU1_L3VPN,INTERNET) source dynamic CU1_L3VPN_NET interface
nat (CU2_L3VPN,INTERNET) source dynamic CU2_L3VPN_NET interface
nat (CU3_L3VPN,INTERNET) source dynamic CU3_L3VPN_NET interface
nat (CU4_L3VPN, INTERNET) source dynamic CU4_L3VPN_NET interface
nat (CU5_L3VPN, INTERNET) source dynamic CU5_L3VPN_NET interface
nat (CU6_L3VPN, INTERNET) source dynamic CU6_L3VPN_NET interface
nat (INTERNAL_10.13.104, INTERNET) source static SPB_ESA1_INT SPB_ESA1_EXT
nat (INTERNAL_10.13.104, INTERNAL_10.13.128.96) source static SPB_WSA1_INT SPB_WSA1_MGMT2
nat (INTERNET, INTERNAL_10.13.104) source static CU6_VPN_POOL CU6_VPN_POOL
nat (INTERNET, CU6_L3VPN) source static CU6_VPN_POOL CU6_VPN_POOL
nat (INTERNET, INTERNAL_10.13.104, INTERNAL) source static CU1_VPN_CLIENTS CU1_VPN_CLIENTS
access-group DMZ_ACL in interface INTERNAL_10.13.104
access-group CU1_L3VPN_ACL in interface CU1_L3VPN
access-group CU2_L3VPN_ACL in interface CU2_L3VPN
access-group CU3_L3VPN_ACL in interface CU3_L3VPN
access-group CU4_L3VPN_ACL in interface CU4_L3VPN
access-group CU5_L3VPN_ACL in interface CU5_L3VPN
access-group CU6_L3VPN_ACL in interface CU6_L3VPN
access-group INTERNET_ACL in interface INTERNET

prefix-list CU1_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU1_INT_ROUTES seq 10 permit 10.13.201.0/24

prefix-list CU2_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU2_INT_ROUTES seq 10 permit 10.13.202.0/24

prefix-list CU3_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU3_INT_ROUTES seq 10 permit 10.13.203.0/24

prefix-list CU4_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU4_INT_ROUTES seq 10 permit 10.13.204.0/24

prefix-list CU5_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU5_INT_ROUTES seq 10 permit 10.13.205.0/24

prefix-list CU6_INT_ROUTES seq 5 permit 10.13.104.0/24
prefix-list CU6_INT_ROUTES seq 10 permit 10.13.206.0/24

prefix-list DMZ_ROUTES seq 10 permit 10.13.11.0/24 ge 31

prefix-list private-routes seq 10 permit 10.13.101.0/24
prefix-list private-routes seq 20 permit 10.13.102.0/24
prefix-list private-routes seq 30 permit 10.13.103.0/24
prefix-list private-routes seq 40 permit 10.13.104.0/24

route-map WSA_PBR permit 10
match ip address WSA_PBR
set ip next-hop 10.13.104.12

router bgp 65513
bgp log-neighbor-changes
address-family ipv4 unicast
neighbor 10.13.9.254 remote-as 109
neighbor 10.13.9.254 activate
neighbor 10.13.9.254 prefix-list DMZ_ROUTES out
neighbor 10.13.105.254 remote-as 109
neighbor 10.13.105.254 activate
neighbor 10.13.105.254 prefix-list CU1_INT_ROUTES out
neighbor 10.13.106.254 remote-as 109
neighbor 10.13.106.254 activate
neighbor 10.13.106.254 prefix-list CU2_INT_ROUTES out
neighbor 10.13.107.254 remote-as 109
neighbor 10.13.107.254 activate
neighbor 10.13.107.254 prefix-list CU3_INT_ROUTES out
neighbor 10.13.108.254 remote-as 109
neighbor 10.13.108.254 activate
neighbor 10.13.108.254 prefix-list CU4_INT_ROUTES out
neighbor 10.13.109.254 remote-as 109
neighbor 10.13.109.254 activate
neighbor 10.13.109.254 prefix-list CU5_INT_ROUTES out
neighbor 10.13.110.254 remote-as 109
neighbor 10.13.110.254 activate
neighbor 10.13.110.254 prefix-list CU6_INT_ROUTES out
redistribute static
no auto-summary
no synchronization
exit-address-family
!
route INTERNET 0.0.0.0 0.0.0.0 10.13.9.254 1
route Null0 10.13.11.71 255.255.255.255 1
route Null0 10.13.11.72 255.255.255.255 1
route MANAGEMENT 64.102.255.40 255.255.255.255 10.13.1.1 1
route MANAGEMENT 171.70.168.183 255.255.255.255 10.13.1.1 1
route MANAGEMENT 173.37.145.8 255.255.255.255 10.13.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.13.1.35 255.255.255.255 MANAGEMENT
http 10.13.1.81 255.255.255.255 MANAGEMENT
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpoint SPB_TRUSTPOINT
  enrollment self
  fqdn vpn.spb.com
  email admin@spb.com
  subject-name CN=vpn
  keypair SSL_VPN_KEY
  proxy-ldc-issuer
crl configure
crypto ca trustpoint CU6_TRUSTPOINT
  enrollment self
  fqdn vpn6.spb.com
  email admin@spb.com
  subject-name CN=vpn6
  keypair CUSTOMER6_KEY
  proxy-ldc-issuer
crl configure
crypto ca trustpoint CU5_TRUSTPOINT
  enrollment self
  fqdn vpn5.spb.com
  email admin@spb.com
  subject-name CN=vpn5
  proxy-ldc-issuer
crl configure
crypto ca trustpoint CU4_TRUSTPOINT
  enrollment self
  fqdn vpn4.spb.com
  email admin@spb.com
Appendix E—HSS SMB Designs Tested

subject-name CN=vpn4
proxy-ldc-issuer
crl configure
crypto ca trustpoint CU3_TRUSTPOINT
   enrollment self
   fqdn vpn3.spb.com
e-mail admin@spb.com
subject-name CN=vpn3
proxy-ldc-issuer
crl configure
crypto ca trustpoint CU2_TRUSTPOINT
   enrollment self
   fqdn vpn2.spb.com
e-mail admin@spb.com
subject-name CN=vpn2
proxy-ldc-issuer
crl configure
crypto ca trustpoint CU1_TRUSTPOINT
   enrollment self
   fqdn vpn1.spb.com
e-mail admin@spb.com
subject-name CN=vpn1
proxy-ldc-issuer
crl configure
no validation-usage
crypto ca trustpool policy
auto-import
crypto ca certificate chain SPB_TRUSTPOINT
certificate dd20c657

subject-name CN=vpn4
proxy-ldc-issuer
crl configure
crypto ca trustpoint CU6_TRUSTPOINT
   enrollment self
   fqdn vpn6.spb.com
e-mail admin@spb.com
subject-name CN=vpn6
proxy-ldc-issuer
crl configure
crypto ca trustpoint _SmartCallHome_ServerCA
   enrollment self
   fqdn spb.com
e-mail admin@spb.com
subject-name CN=spb.com
proxy-ldc-issuer
crl configure
Appendix E—HSS SMB Designs Tested

167
Cisco Hosted Security as a Service

quit
telnet timeout 5
ssh stricthostkeycheck
ssh 10.13.1.35 255.255.255.255 MANAGEMENT
ssh 10.13.1.81 255.255.255.255 MANAGEMENT
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp authentication-key 1 md5 Cicco123
ttp authenticate
ntp trusted-key 1
ntp server 10.13.1.20 key 1 source MANAGEMENT prefer
webvpn
enable INTERNET
anyconnect image disk0:/anyconnect-win-4.1.00028-k9.pkg 1
anyconnect profiles CU1_AC_PROFILE disk0:/CU1_AC_PROFILE.xml
anyconnect profiles CU2_AC_PROFILE disk0:/CU2_AC_PROFILE.xml
anyconnect profiles CU3_AC_PROFILE disk0:/CU3_AC_PROFILE.xml
anyconnect profiles CU4_AC_PROFILE disk0:/CU4_AC_PROFILE.xml
anyconnect profiles CU5_AC_PROFILE disk0:/CU5_AC_PROFILE.xml
anyconnect profiles CU6_AC_PROFILE disk0:/CU6_AC_PROFILE.xml
anyconnect enable
cache
disable
error-recovery disable
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ssl-client
group-policy CU1_GRP_POLICY internal
group-policy CU1_GRP_POLICY attributes
banner value Welcome to Customer 1 VPN
wins-server none
dns-server value 10.13.16.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer1.com
split-tunnel-all-dns enable
address-pools value CU1_VPN_POOL
webvpn
anyconnect profiles value CU1_AC_PROFILE type user
customization value CU1_CUSTOM_OBJ
group-policy CU1_GRP_POLICY internal
group-policy CU3_GRP_POLICY attributes
banner value Welcome to Customer 3 VPN
wins-server none
dns-server value 10.13.48.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer3.com
split-tunnel-all-dns enable
address-pools value CU3_VPN_POOL
webvpn
  anyconnect profiles value CU3_AC_PROFILE type user
customization value CU3_CUSTOM_OBJ


group-policy CU2_GRP_POLICY internal
group-policy CU2_GRP_POLICY attributes
  banner value Welcome to Customer 2 VPN
wins-server none
dns-server value 10.13.32.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer2.com
split-tunnel-all-dns enable
address-pools value CU2_VPN_POOL
webvpn
  anyconnect profiles value CU2_AC_PROFILE type user
customization value CU2_CUSTOM_OBJ

group-policy CU5_GRP_POLICY internal
group-policy CU5_GRP_POLICY attributes
  banner value Welcome to Customer 5 VPN
wins-server none
dns-server value 10.13.80.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer5.com
split-tunnel-all-dns enable
address-pools value CU5_VPN_POOL
webvpn
  anyconnect profiles value CU5_AC_PROFILE type user
customization value CU5_CUSTOM_OBJ

group-policy CU4_GRP_POLICY internal
group-policy CU4_GRP_POLICY attributes
  banner value Welcome to Customer 4 VPN
wins-server none
dns-server value 10.13.64.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer4.com
split-tunnel-all-dns enable
address-pools value CU4_VPN_POOL
webvpn
  anyconnect profiles value CU4_AC_PROFILE type user
customization value CU4_CUSTOM_OBJ

group-policy CU6_GRP_POLICY internal
group-policy CU6_GRP_POLICY attributes
  banner value Welcome to Customer 6 VPN
wins-server none
dns-server value 10.13.96.5
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelall
default-domain value customer6.com
split-tunnel-all-dns enable
address-pools value CU6_VPN_POOL
webvpn
  anyconnect profiles value CU6_AC_PROFILE type user
customization value CU6_CUSTOM_OBJ
dynamic-access-policy-record DfltAccessPolicy
username admin password c6jy9W/xbkzywfpb encrypted privilege 15
username vpn-user6 password GSvCHLtMHKU2dNhd
encrypted
username vpn-user6 attributes
vpn-group-policy CU6_GRP_POLICY
vpn-filter value CU6_VPN_CLIENTS_ACL
vpn-tunnel-protocol ssl-client ssl-clientless
service-type remote-access
username vpn-user4 password GSvCHLtMHKU2dNhd
encrypted
username vpn-user4 attributes
vpn-group-policy CU4_GRP_POLICY
vpn-filter value CU4_VPN_CLIENTS_ACL
vpn-tunnel-protocol ssl-client ssl-clientless
service-type remote-access
username vpn-user5 password GSvCHLtMHKU2dNhd
encrypted
username vpn-user5 attributes
vpn-group-policy CU5_GRP_POLICY
vpn-filter value CU5_VPN_CLIENTS_ACL
vpn-tunnel-protocol ssl-client ssl-clientless
service-type remote-access
username vpn-user2 password GSvCHLtMHKU2dNhd
encrypted
username vpn-user2 attributes
vpn-group-policy CU2_GRP_POLICY
vpn-filter value CU2_VPN_CLIENTS_ACL
vpn-tunnel-protocol ssl-client ssl-clientless
service-type remote-access
username vpn-user3 password GSvCHLtMHKU2dNhd
encrypted
username vpn-user3 attributes
vpn-group-policy CU3_GRP_POLICY
vpn-filter value CU3_VPN_CLIENTS_ACL
vpn-tunnel-protocol ssl-client ssl-clientless
service-type remote-access
tunnel-group CU1_AC_PROFILE type remote-access
address-pool CU1_VPN_POOL
default-group-policy CU1_GRP_POLICY
tunnel-group CU1_AC_PROFILE general-attributes
customization CU1_CUSTOM_OBJ
group-alias 1 disable
group-alias Customer disable
group-alias Customer1 disable
group-url https://vpn.customer1.com enable
group-url https://vpn.spb.com/customer1 enable
dns-group CU1_DNS
tunnel-group CU2_AC_PROFILE type remote-access
address-pool CU2_VPN_POOL
default-group-policy CU2_GRP_POLICY
dhcp-server 10.13.32.5
tunnel-group CU2_AC_PROFILE general-attributes
customization CU2_CUSTOM_OBJ
radius-reject-message
proxy-auth sdi
group-alias Customer2 disable
group-url https://vpn.customer2.com enable
group-url https://vpn.spb.com/customer2 enable
dns-group CU2_DNS
tunnel-group CU3_AC_PROFILE type remote-access
tunnel-group CU3_AC_PROFILE general-attributes
address-pool CU3_VPN_POOL
default-group-policy CU3_GRP_POLICY
dhcp-server 10.13.48.5
tunnel-group CU3_AC_PROFILE webvpn-attributes
  customization CU3_CUSTOM_OBJ
  radius-reject-message
  proxy-auth sdi
  group-alias Customer3 disable
  group-url https://vpn.customer3.com enable
dns-group CU3_DNS
tunnel-group CU4_AC_PROFILE type remote-access
tunnel-group CU4_AC_PROFILE general-attributes
  address-pool CU4_VPN_POOL
default-group-policy CU4_GRP_POLICY
dhcp-server 10.13.64.5
tunnel-group CU4_AC_PROFILE webvpn-attributes
  customization CU4_CUSTOM_OBJ
  radius-reject-message
  proxy-auth sdi
  group-alias Customer4 disable
  group-url https://vpn.customer4.com enable
dns-group CU4_DNS
tunnel-group CU5_AC_PROFILE type remote-access
tunnel-group CU5_AC_PROFILE general-attributes
  address-pool CU5_VPN_POOL
default-group-policy CU5_GRP_POLICY
dhcp-server 10.13.80.5
tunnel-group CU5_AC_PROFILE webvpn-attributes
  customization CU5_CUSTOM_OBJ
  radius-reject-message
  proxy-auth sdi
  group-alias Customer5 disable
  group-url https://vpn.customer5.com enable
dns-group CU5_DNS
tunnel-group CU6_AC_PROFILE type remote-access
tunnel-group CU6_AC_PROFILE general-attributes
  address-pool CU6_VPN_POOL
default-group-policy CU6_GRP_POLICY
dhcp-server 10.13.96.5
tunnel-group CU6_AC_PROFILE webvpn-attributes
  customization CU6_CUSTOM_OBJ
  radius-reject-message
  proxy-auth sdi
  group-alias Customer6 disable
  group-url https://vpn.customer6.com enable
dns-group CU6_DNS

! class-map inspection_default
  match default-inspection-traffic
  !
 policy-map type inspect dns migrated_dns_map_1
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
 policy-map global_policy
  class inspection_default
    inspect dns migrated_dns_map_1
    inspect ftp
    inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
http-proxy 64.102.255.40 port 80
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
profile License
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
Cryptochecksum:d72c05a65559272096024945b682e5bc8
: end
**Appendix E—HSS SMB Designs Tested**

**SMB Design 2b—ASAv, Shared ESAv, Shared WSAv, Private AMP Dedicated and Private AMP Threat Grid**

Refer to SMB Design 1b for the ASAv configuration.