SAFE Design Guide

Secure Internet Edge: Remote Access VPN with DDoS

September 2016

SAFE
SIMPLIFIES SECURITY

Contents

Introduction

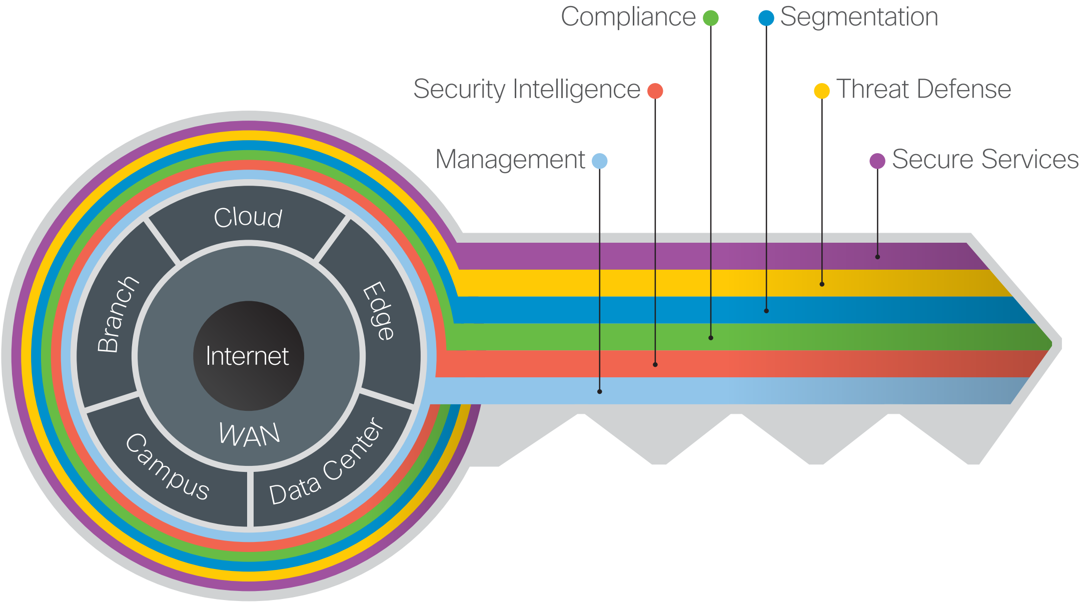
This guide addresses a specific use case of remote access VPN connections covered in the SAFE Edge Architecture guide. The design validation for remote access VPN connections includes Distributed Denial of Service (DDoS) protections utilizing the Radware decorator application.

An important segment of an enterprise network is the Internet edge, where the corporate network meets the public Internet. As your network users reach out to websites and use email and other collaboration tools for business-to-business communication, the resources of the corporate network must remain both accessible and secure.

The SAFE Model identifies the Internet edge as one of the places in the network (PINs). SAFE simplifies complexity across the enterprise by implementing a model that focuses on the areas that a company must secure. This model treats each area holistically, focusing on today's threats and the capabilities needed to secure each area against those threats. Cisco has deployed, tested, and validated critical challenges.

These solutions provide guidance, complete with configuration steps that ensure effective, secure deployments for our customers.

The Internet edge is the highest-risk PIN because it is the primary ingress for public traffic and the primary egress point to the Internet. Simultaneously, it is the critical resource that businesses need in today's Internet-based economy. SAFE matches up defensive capabilities against the categories of threats today.



The Key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domains.

Internet Edge RA VPN

Employees, contractors, and partners often need to access the network when traveling or working from home or other offsite locations.

Many organizations therefore need to provide users in remote locations with network connectivity to data resources.

A secure connectivity solution for the Internet edge should support:

- A wide variety of endpoint devices
- Seamless access to networked data resources
- Authentication and policy control that integrates with the authentication resources used by the organization
- Cryptographic security to prevent sensitive data from exposure to unauthorized parties who accidentally or intentionally intercept the data

Designs for the Internet edge address these needs with the Cisco ASA/Firepower family and Cisco AnyConnect Secure Mobility Client. The Remote Access Virtual Private Network (RA VPN) zone implements dedicated resources to connect remote users and sites.

This design guide focuses on the remote access use case within the Internet edge PIN, which is one of the six use case flows outlined in the SAFE Edge Architecture Guide. It does not include items such as client security, load balancing, or server security. These are covered in other guides.

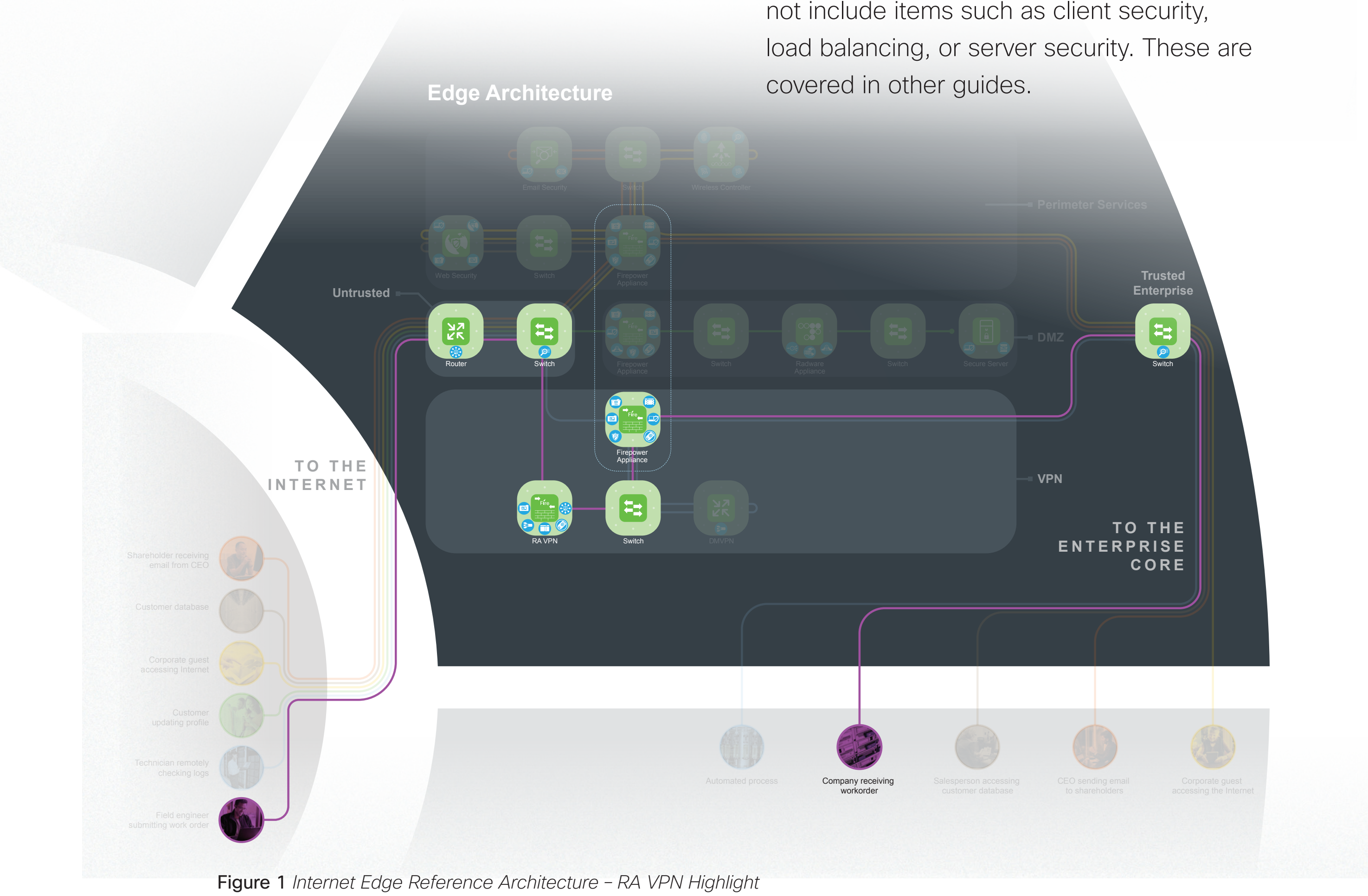


Figure 1 *Internet Edge Reference Architecture – RA VPN Highlight*

Internet Edge RA VPN Design

This design for the Internet edge implements remote access VPN deployed on a pair of Cisco Firepower 9300 appliances configured to use the ASA image for high availability and remote access VPN. The Radware DefensePro Distributed Denial of Service (DDoS) decorator application (vDP on the FP9300) was also installed to provide additional protection of these VPN termination points. The design adds a second pair of Cisco ASA appliances using the Firepower Threat Defense (FTD) software image, and configured for high availability to perform the services of Next-Generation Intrusion Prevention (NGIPS) in addition to next-generation firewalling (NGFW) for inspection of the remote users sessions after tunnel termination. This design offers greater visibility, scalability, and security while providing a simple migration path from an existing RA VPN installations.

From the proposed architecture and use case above, we implemented this detailed design for validating the Remote Access VPN use case. The purple line indicates the RA VPN communication flow through the design.

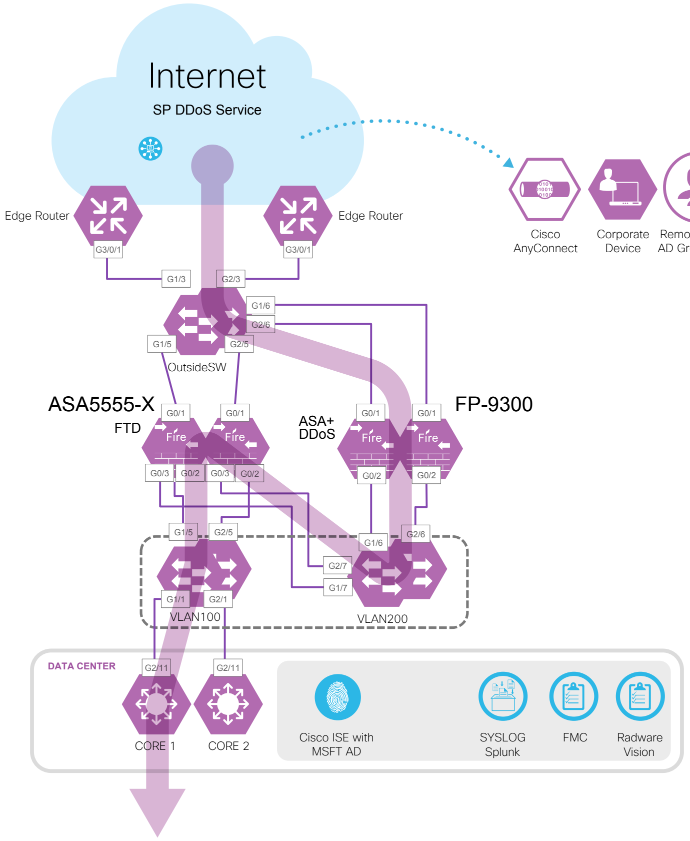


Figure 2 *High-Level Internet Edge RA VPN Design Flow*

Implementation

The following sub sections provide information on how each of the devices were configured and references to supporting configuration documentation. They represent Cisco best practices for this design. Full device configurators are provided in the accompanying appendix for devices with CLI interfaces and easily listable configurations.

Table 1 *Validated Components*

Component	Role	Hardware	Release
Cisco Firepower Next-Generation Firewall (NGFW) Appliance	Remote access headend firewall	Firepower 9300 with FPR9K-SM-36 running ASA image	Firepower Chassis Manager Ver.1.1(4.85g) Cisco ASA Software Release 9.6(0)124
Radware Virtual Defense Pro	Manages DDoS protection	Virtual module within FP 9300	Radware VDP ver 1.01.02
Cisco AnyConnect VPN Client	Remote Access VPN Client	N/A installed in the remote client, PC, Mac®, and iPhone®	Version 4.2.02075
Cisco Adaptive Security Appliance (ASA)	Edge NGFW Security	ASA5555-X Firepower Threat Defense	FTD6.0.1
Firepower Management Console	Edge intrusion policy management	FMC-3500	6.0.1 (build 1213)
Cisco Identity Services Engine (ISE)	Roles-based policy management / authentication server	Virtual machine (VMware)	Version 2.0.0.306
Radware Vision Console	DDoS profile management and tuning	APSolute Vision VA	Version 3.330
Edge Routers	Internet gateway	ASR1002-X	15.3(1)S
Edge Switches	Access switch	C9372PX	nxos.7.0.3.I2.2b.bin
Cisco Nexus 7000	Aggregation and FlexPod access switch	Cisco Nexus 7004 Cisco Nexus 7010	NX-OS version 6.1(2)
Radware-Raptor Attack Tool	DDoS attacks	VM	Version 2.6.37

Edge Routers

The external edge router provides connectivity from the service provider to the enterprise. Internet edge best practices are to implement basic filtering on the external and internal interfaces to block spoofed and undesired traffic, careful to match your organization's environment (e.g., block RFC 1918 networks and your own Internet subnets, inbound from the Internet).

The devices are configured for AAA role-based authentication to the corporate Identity Services Engine using TACACS+.

Logs are sent to a centralized logging collection server. Device time is synchronized to know and trusted time sources.

To meet various compliance regulations; login banners and interface access lists are implemented to restrict administrative access to the system. And only secure protocols are enable and used.

The edge routers are deployed in a high-availability pair using HSRP in the internal interfaces.

Large organizations will typically implement external border gateway routing protocols to advertise their owned IP space. These configurations are beyond the scope of this use case. For simplicity of this validation, static routes were used.

Coarse Filtering Example

```
interface GigabitEthernet0/0/1
 ip access-group INTERNAL-FILTER-IN in

interface GigabitEthernet0/0/3
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out

ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
```

Coarse Filtering Example, continued

```
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 10.11.206.0 0.0.0.255 log
 deny   ip any 1.1.1.0 0.0.0.255 log
 remark -
 remark ---Block Spoofing of your networks---
 remark enter your IP block here
 remark ---Permit all other traffic---
 permit ip any any
```

Role-based Authentication Example

```
aaa new-model
aaa group server tacacs+ PRIMARY1
 server name PRIMARY
 ip tacacs source-interface GigabitEthernet0/0/1
!
aaa authentication login COMPLIANCE group PRIMARY1 local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+

aaa session-id common

tacacs server PRIMARY
 address ipv4 10.11.230.111
 key 7 <removed>
```

Centralized Logging Example

```
logging buffered 50000 informational
no logging rate-limit

login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log

archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys

logging trap informational
logging source-interface GigabitEthernet0/0/1
logging host 10.11.230.161
```

Time Synchronization Example

```
clock timezone PST -8 0
clock summer-time PST recurring

ntp authentication-key 555 md5 mysecretkey
ntp trusted-key 555
ntp authenticate
ntp source GigabitEthernet0/0/3
ntp server 171.68.10.80 prefer
ntp server 171.68.10.150
```

Secure Management Protocols Example

```
ip ssh version 2
ip scp server enable
no service pad
no ip http server
no ip http secure-server

line vty 0 15
 session-timeout 15  output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication COMPLIANCE
 transport input ssh
```

A complete device running configuration is available in the appendix.

Edge Switches

The edge switches provide connectivity between the various DMZ systems. Two pair of Nexus 9000 Series switches were selected, as they are typically the most affordable 10G ports for the services needed.

Security best practices are to only implement Layer 2 switching in this environment so as to not expose any system resources. Only the management interface is used via an out-of-band network for access, configuration, and monitoring.

The devices are configured for AAA role-based authentication to the corporate Identity Services Engine using TACACS+.

Netflow and logs are sent to centralized logging/collection servers. Device time is synchronized to known and trusted time sources. To meet various compliance regulations, login banners and interface access lists are implemented to restrict administrative access to the system. And only secure protocols are enabled and used.

The switches are deployed in a high availability pair, one pair external and one pair as a DMZ segment. All unused interfaces are shut down.

Role-based Authentication Example

```
feature tacacs+

tacacs-server key 7 “<removed>”
tacacs-server host 10.11.230.111
aaa group server tacacs+ CiscoISE
    server 10.11.230.111
    use-vrf management
    source-interface mgmt0
aaa group server tacacs+ tacacs
feature password encryption aes

aaa authentication login default group CiscoISE
aaa authentication login console group CiscoISE
aaa authorization ssh-certificate default group CiscoISE
aaa accounting default group CiscoISE
aaa authentication login error-enable
```

Centralized Logging and NetFlow Example

```
logging server 10.11.230.161 5 use-vrf management
logging source-interface mgmt0

feature sflow
sflow sampling-rate 50000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 10.11.230.154 vrf management
sflow collector-port 7000
sflow agent-ip 10.11.230.154
sflow data-source interface ethernet 1/1-7

hardware access-list tcam region sflow 256
```

Time Synchronization Example

```
clock timezone PST -8 0
clock summer-time PDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60

ntp server 10.11.255.1 prefer use-vrf management
ntp server 10.11.255.2 use-vrf management
ntp server 172.26.129.252 use-vrf management
ntp server 172.28.189.1 use-vrf management
ntp source-interface  mgmt0
```

Secure Management Protocols Example

```
!NexOS only uses SSHv2, and does not have HTTP/s, other protocols disabled by default

ssh key rsa 2048

line vty
  exec-timeout 15
  logout-warning 20
  access-class SwitchMgmt in
```

A complete device running configuration is available in the Appendix.
Additional Nexus 9000 Series configuration information can be found here: https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html

RA VPN Security Appliances

The topology for Remote Access VPN for Internet edge design includes at least two Firepower 9300 or 4100 security appliances running ASA software, with Radware DDoS Virtual Defense Pro as a decorator application image deployed as active/standby high availability setup.

The connection among switches and inter-chassis high availability connections are 10 Gbps interfaces.

The ASA configuration is performed via CLI, Cisco Adaptive Security Device Manager (ASDM), or Cisco Security Manager (CSM). Policies for the firewalls are easily managed via ADSM or CSM. User/server device objects are managed in Cisco Identity Services Engine (ISE) along with TrustSec policy creation for remaining platforms. User accounts and authentication are linked to Active Directory via the Identity Services Engine (ISE).

Cisco ASA Firewall Remote Access

AnyConnect

AnyConnect Secure Mobility Client increases visibility and control across the extended network, preventing compromised endpoints from gaining access to critical resources. It:

- Selects the most efficient tunneling protocols for the application
- Offers advanced Layer 2 access to facilitate simultaneous device and user authentication
- Grants access to select enterprise applications remotely for tablets and smartphones
- Serves as the agent for posture to deliver consistent, highly secure endpoint access across wired, wireless, and VPN
- Provides optional web security and advanced malware threat defense
- Monitors endpoint application usage to help expose suspicious behaviors

AnyConnect delivers context-aware, comprehensive, and simplified security policy enforcement with the Cisco Identity Services Engine (ISE).

You can also use it to assist with the deployment of Cisco Advanced Malware Protection (AMP) for Endpoints. Its AMP Enabler capability expands endpoint threat protection to VPN-enabled endpoints or wherever Cisco AnyConnect services are in use.

New with Cisco AnyConnect 4.2 is the Network Visibility module on Windows® and Mac OS® X platforms. Administrators can now monitor endpoint application usage to uncover potential behavior anomalies and to make more informed network design decisions. Usage data can be shared with a growing number of Internet Protocol Information Export (IPFIX) capable network analysis tools.

Note: Although AnyConnect supports a variety of security functions, we focused only on the deployment of the AnyConnect VPN functionality to the Firepower 9300 running an ASA image as the VPN termination device.

The links below provide basic CLI and ASA configuration guidance.

- ASA 9.6 CLI configuration guide: https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html

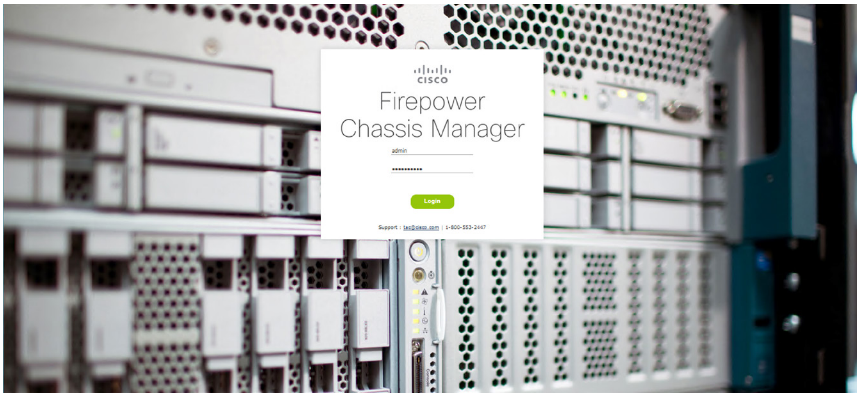
- Additional ASA configuration guides: https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

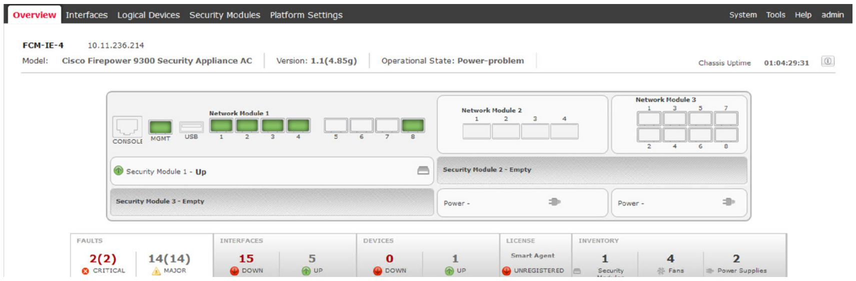
Initial Setup of Firepower 9300

Step 1 Set up management IP address

Upon receiving the FP9300 unit, use console port to initialize the setup to specify the FXOS management IP address. Note this is interdependent of the management IP address you will specify for the ASA management interface.

Using the FXOS management IP address, you can access its GUI to configure most of the hardware settings and interface mappings.





FCM-IE-4 10.11.236.214

Model: Cisco Firepower 9300 Security Appliance AC | Version: 1.1(4.85g) | Operational State: Power-problem Chassis Uptime 01:04:29:31

Security Module 1 - Up

Security Module 2 - Empty

Security Module 3 - Empty

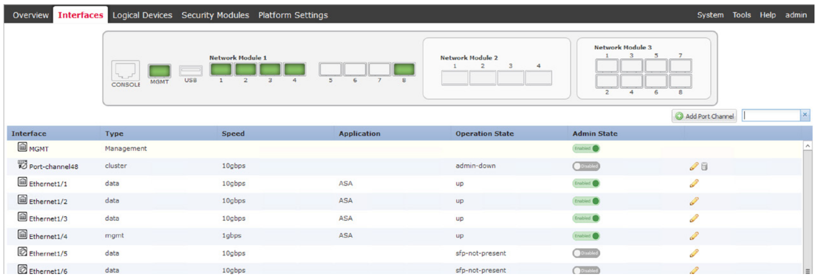
FAULTS: 2(2) CRITICAL, 14(14) MAJOR | INTERFACES: 15 DOWN, 5 UP | DEVICES: 0 DOWN, 1 UP | LICENSE: Smart Agent UNREGISTERED | INVENTORY: 1 Security Modules, 4 Fans, 2 Power Supplies

Initial Setup of Firepower 9300, continued

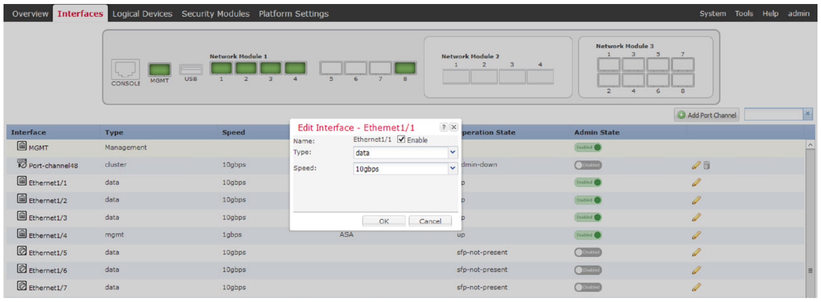
Step 2 Interface configuration and its allocation

Select the Interface tab to enable associated interfaces.

You can either configure it as Data or Management interface.



Interface	Type	Speed	Application	Operation State	Admin State
MGMT	Management				Enabled
Port-channel48	cluster	10gbps		admin-down	Disabled
Ethernet1/1	data	10gbps	ASA	up	Enabled
Ethernet1/2	data	10gbps	ASA	up	Enabled
Ethernet1/3	data	10gbps	ASA	up	Enabled
Ethernet1/4	mgmt	1gbps	ASA	up	Enabled
Ethernet1/5	data	10gbps		sfp-not-present	Disabled
Ethernet1/6	data	10gbps		sfp-not-present	Disabled



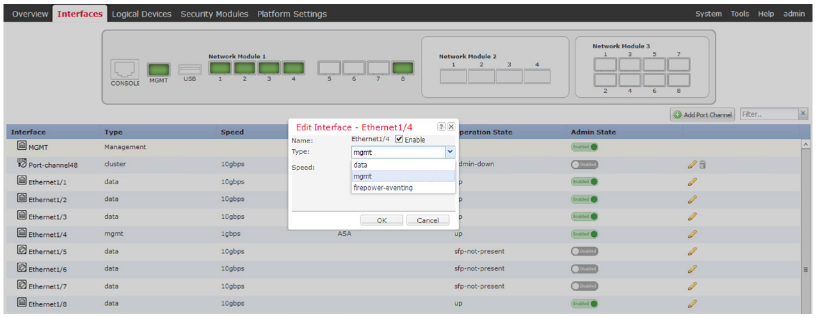
Edit Interface - Ethernet1/1

Name: Ethernet1/1 ☑ Enable

Type: data

Speed: 10gbps

Interface	Type	Speed		peration State	Admin State
MGMT	Management				Enabled
Port-channel48	cluster	10gbps		dmin-down	Disabled
Ethernet1/1	data	10gbps		p	Enabled
Ethernet1/2	data	10gbps		p	Enabled
Ethernet1/3	data	10gbps		p	Enabled
Ethernet1/4	mgmt	1gbps	ASA	up	Enabled
Ethernet1/5	data	10gbps		sfp-not-present	Disabled
Ethernet1/6	data	10gbps		sfp-not-present	Disabled
Ethernet1/7	data	10gbps		sfp-not-present	Disabled



Edit Interface - Ethernet1/4

Name: Ethernet1/4 ☑ Enable

Type: mgmt

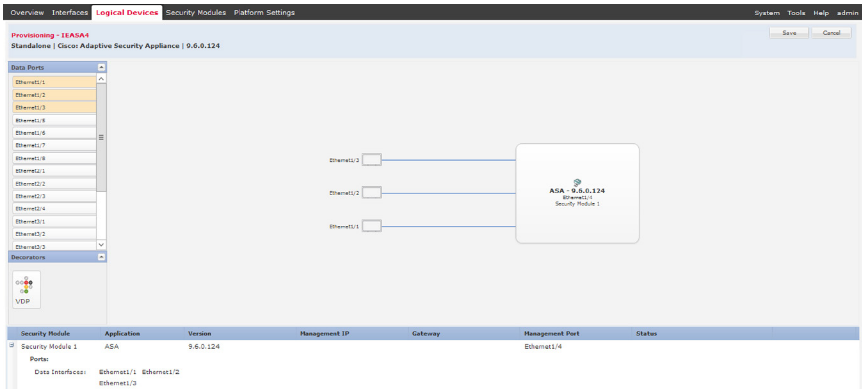
Speed:

Interface	Type	Speed		peration State	Admin State
MGMT	Management				Enabled
Port-channel48	cluster	10gbps		dmin-down	Disabled
Ethernet1/1	data	10gbps		p	Enabled
Ethernet1/2	data	10gbps		p	Enabled
Ethernet1/3	data	10gbps		p	Enabled
Ethernet1/4	mgmt	1gbps	ASA	up	Enabled
Ethernet1/5	data	10gbps		sfp-not-present	Disabled
Ethernet1/6	data	10gbps		sfp-not-present	Disabled
Ethernet1/7	data	10gbps		sfp-not-present	Disabled
Ethernet1/8	data	10gbps		up	Enabled

Initial Setup of Firepower 9300, continued

Step 3 Allocate interfaces to logical devices

Select Logical Device Tab then select the interfaces you wish to be allocated to the logical device.

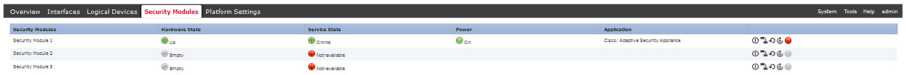


Provisioning - IEASA4
Standalone | Cisco: Adaptive Security Appliance | 9.6.0.124

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	ASA	9.6.0.124			Ethernet1/4	

Ports:
Data Interfaces: Ethernet1/1 Ethernet1/2 Ethernet1/3

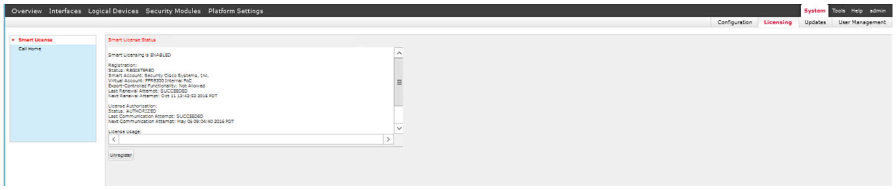
If you do not see the logical device, select the Security Module tab to make sure the module is powered up and enabled.



Security Modules	Hardware State	Service State	Power	Application	
Security Module 1	Up	Online	On	Cisco: Adaptive Security Appliance	
Security Module 2	Empty	Not-available			
Security Module 3	Empty	Not-available			

Step 4 Enable license

Select System tab->Licensing to access the Smart Licensing page where you can input the license token to enable the features. Note: To access ASDM, 3DES license needs to be recognized by Smart License Server.



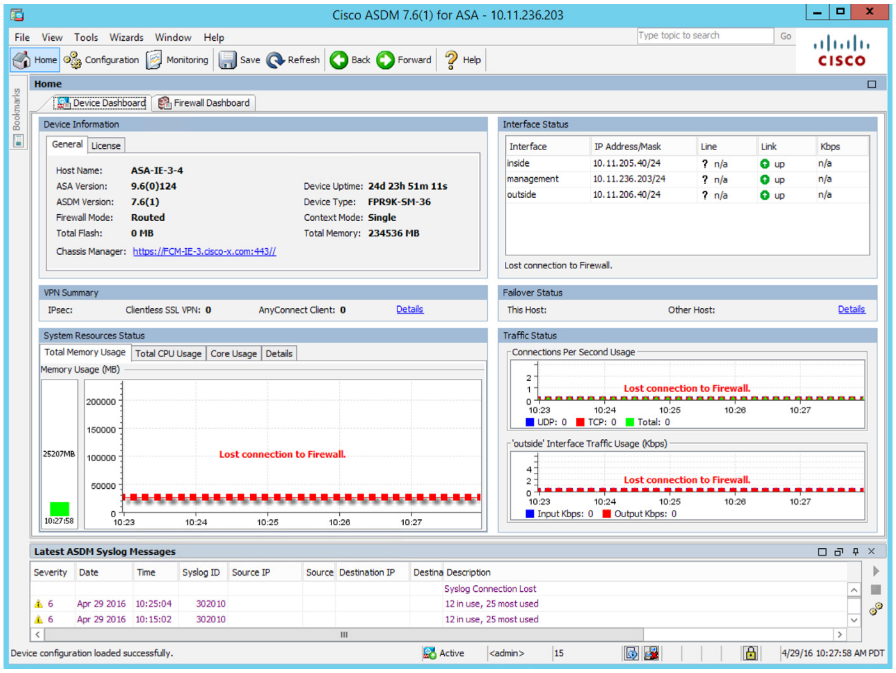
Smart License Status

```
Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: Security Cisco Systems, Inc.
Virtual Account: FPR9300 Internal PoC
Export-Controlled Functionality: Not Allowed
Last Renewal Attempt: SUCCEEDED
Next Renewal Attempt: Oct 11 13:42:53 2016 PDT

License Authorization:
Status: AUTHORIZED
Last Communication Attempt: SUCCEEDED
Next Communication Attempt: May 06 09:04:40 2016 PDT

License Usage:
```

Initial Setup of Firepower 9300, continued

Step 5 Initiate ASDM to configure VPN and firewall using the VPN wizard for AnyConnect VPNs.

Instructions for the VPN wizard are available here: http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asdm76/vpn/asdm-76-vpn-config/vpn-wizard.html#ID-2217-0000005b



Device Information

Host Name: ASA-IE-3-4
ASA Version: 9.6(0)124
ASDM Version: 7.6(1)
Firewall Mode: Routed
Total Flash: 0 MB
Device Uptime: 24d 23h 51m 11s
Device Type: FPR9K-SM-36
Context Mode: Single
Total Memory: 234536 MB
Chassis Manager: https://FCM-IE-3.cisco-x.com:443//

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
inside	10.11.205.40/24	? n/a	up	n/a
management	10.11.236.203/24	? n/a	up	n/a
outside	10.11.206.40/24	? n/a	up	n/a

Lost connection to Firewall.

VPN Summary

IPsec: Clientless SSL VPN: 0 AnyConnect Client: 0 Details

Failover Status

This Host: Other Host: Details

System Resources Status

Traffic Status

Latest ASDM Syslog Messages

Severity	Date	Time	Syslog ID	Source IP	Source	Destination IP	Destina	Description
								Syslog Connection Lost
⚠ 6	Apr 29 2016	10:25:04	302010					12 in use, 25 most used
⚠ 6	Apr 29 2016	10:15:02	302010					12 in use, 25 most used

Device configuration loaded successfully. Active <admin> 15 4/29/16 10:27:58 AM PDT

Initial Setup of Firepower 9300, continued

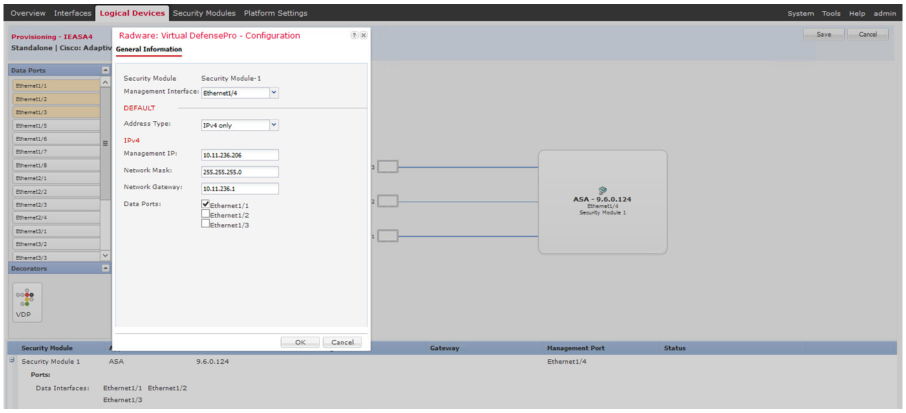
Step 6 Install Radware vDP

Download Radware vDP into devices disk.

Edit ASA Logical Device.

On the left column, select vDP icon to configure vDP as follow. Select one of the data ports which you wish to be associated with vDP.

Note: Management interfaces can be the same interface as the ASA management interface, but a different IP address is required.



Radware: Virtual DefensePro - Configuration

General Information

Security Module: Security Module-1
Management Interface: Ethernet1/4

DEFAULT

Address Type: IPv4 only

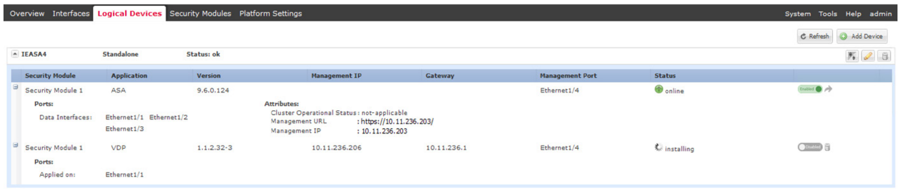
IPv4

Management IP: 10.11.236.206
Network Mask: 255.255.255.0
Network Gateway: 10.11.236.1
Data Ports:
☑ Ethernet1/1
□ Ethernet1/2
□ Ethernet1/3

Security Module	A			Gateway	Management Port	Status
Security Module 1	ASA	9.6.0.124			Ethernet1/4	

Ports:
Data Interfaces: Ethernet1/1 Ethernet1/2 Ethernet1/3

vDP will start the installation process.



IEASA4 Standalone Status: ok

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	ASA	9.6.0.124			Ethernet1/4	online
Security Module 1	VDP	1.1.2.32-3	10.11.236.206	10.11.236.1	Ethernet1/4	installing

ASA — Ports: Data Interfaces: Ethernet1/1 Ethernet1/2 Ethernet1/3

Attributes:
Cluster Operational Status : not-applicable
Management URL : https://10.11.236.203/
Management IP : 10.11.236.203

VDP — Ports: Applied on: Ethernet1/1

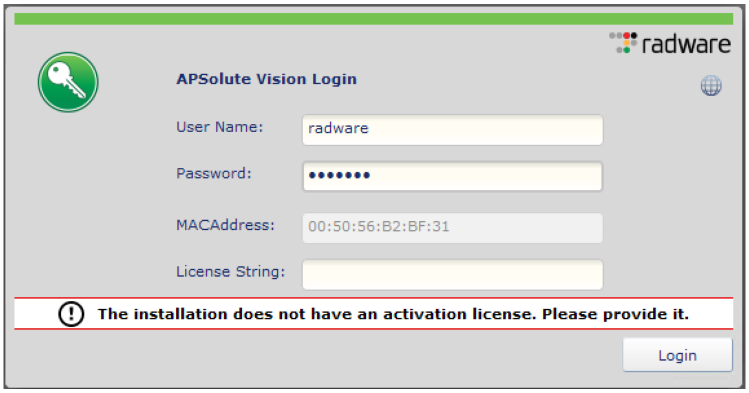
Initial Setup of Firepower 9300, continued

Step 7 Install Vision

Vision is the management server to for vDP. In this document, we have installed the virtual image on a VMWare hypervisor.

After the installation, you can access Vision from browser. Upon log in, you will be asked to input the license string provided by Radware.

The default user name and password is radware/radware.



APSolute Vision Login

User Name: radware

Password: •••••••

MACAddress: 00:50:56:B2:BF:31

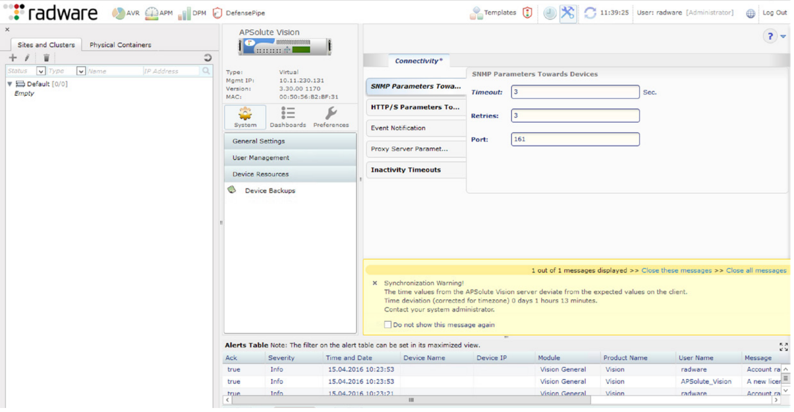
License String:

The installation does not have an activation license. Please provide it.

Step 8 Add vDP into Vision and configure

On the Vision screen under Sites and Clusters, select the "+" icon to add a device.

Select DefensePro from the drop down list and set name, management IP address, SNMP version, and other necessary information.



Type: Virtual
Mgmt IP: 10.11.230.131
Version: 3.30.00 1170
MAC: 00:50:56:B2:BF:31

SNMP Parameters Towards Devices

Timeout: 3 Sec.

Retries: 3

Port: 161

1 out of 1 messages displayed >> Close these messages >> Close all messages

Synchronization Warning!
The time values from the APSolute Vision server deviate from the expected values on the client.
Time deviation (corrected for timezone) 0 days 1 hours 13 minutes.
Contact your system administrator.

□ Do not show this message again

Alerts Table Note: The filter on the alert table can be set in its maximized view.

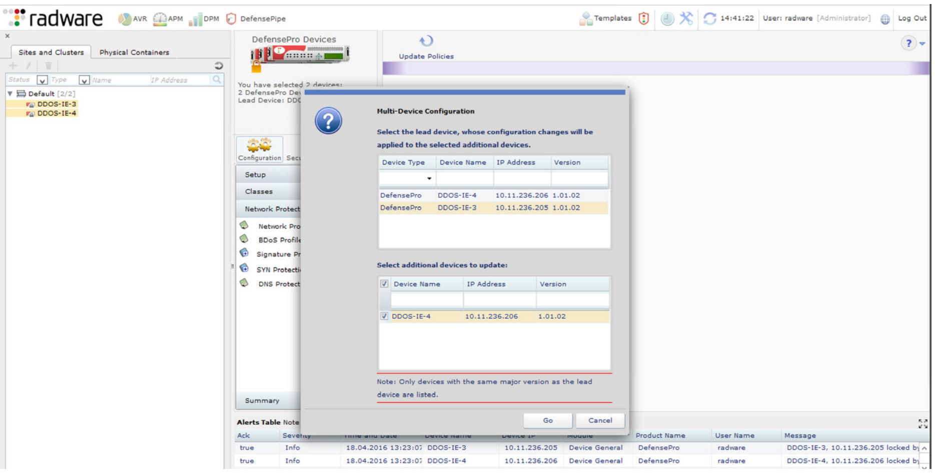
Ack	Severity	Time and Date	Device Name	Device IP	Module	Product Name	User Name	Message
true	Info	15.04.2016 10:23:53			Vision General	Vision	radware	Account ra
true	Info	15.04.2016 10:23:53			Vision General	Vision	APSolute_Vision	A new licer
true	Info	15.04.2016 10:23:21			Vision General	Vision	radware	Account ra

Initial Setup of Firepower 9300, continued

Step 9 Multiple device configuration setup

Although two ASA devices are in high availability status of active/standby, vDP runs independently. Vision has a function to bind multiple devices as one, saving the administrator from configuring multiple devices.

On the Sites and Cluster tab, select multiple vDP (DDoS-IE-3 and DDoS-IE4 in example), and click the arrow button to renew the screen. Selecting the Configuration button will bring up the Multi-Device Configuration windows to select the lead device and other device/s to be updated. Select Go to enable Multi-Device Mode.



Multi-Device Configuration

Select the lead device, whose configuration changes will be applied to the selected additional devices.

Device Type	Device Name	IP Address	Version
DefensePro	DDOS-IE-4	10.11.236.206	1.01.02
DefensePro	DDOS-IE-3	10.11.236.205	1.01.02

Select additional devices to update:

☑	Device Name	IP Address	Version
☑	DDOS-IE-4	10.11.236.206	1.01.02

Note: Only devices with the same major version as the lead device are listed.

Go Cancel

Alerts Table

Ack	Severity	Time and Date	Device Name	Device IP	Module	Product Name	User Name	Message
true	Info	18.04.2016 13:23:07	DDOS-IE-3	10.11.236.205	Device General	DefensePro	radware	DDOS-IE-3, 10.11.236.205 locked by
true	Info	18.04.2016 13:23:07	DDOS-IE-4	10.11.236.206	Device General	DefensePro	radware	DDOS-IE-4, 10.11.236.206 locked by

For further vDP configuration, please refer to Radware’s vDP configuration guides and startup guide.

Edge Security Appliances

Cisco ASA 5555-X with Firepower Threat Defense

In our validation, we implemented two ASA5555-Xs in high-availability mode running the Firepower Threat Defense OS image.

These systems were upgraded from ASA with Firepower services following the steps in this quick start guide: http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html

Configure FTD High Availability

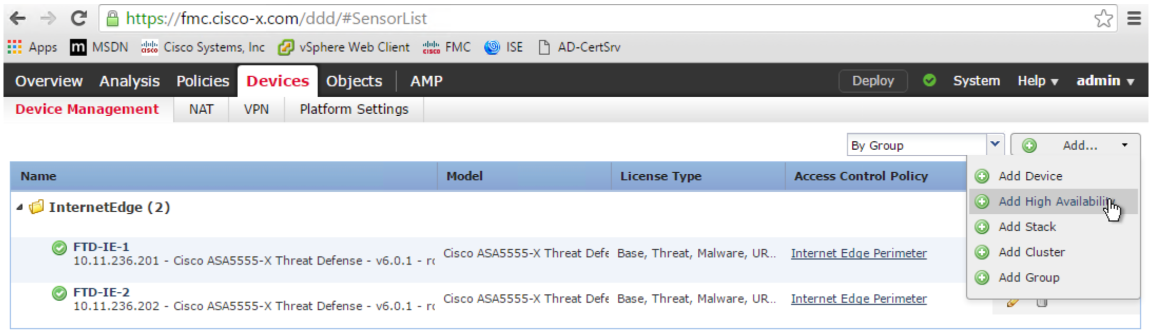
Once the systems were upgraded and added to the Firepower Management Center (FMC), we proceeded to configure the new appliances following the High Availability Deployment section of the Firepower Management Center Configuration Guide, Version 6.0.1: http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601.html

The following details the implementation steps for configuring high availability.

Step 1 Connect Failover and State link interfaces between the two appliances using two crossover cables. For this validation, G0/6 and G0/7 interfaces were utilized. (See lab diagram in appendix.)

Step 2 In FMC, choose Devices > Device Management

Step 3 From the Add drop-down menu on the top right, choose Add High Availability



Name	Model	License Type	Access Control Policy
InternetEdge (2)			
FTD-IE-1 10.11.236.201 - Cisco ASA5555-X Threat Defense - v6.0.1 - r	Cisco ASA5555-X Threat Defe	Base, Threat, Malware, UR..	Internet Edge Perimeter
FTD-IE-2 10.11.236.202 - Cisco ASA5555-X Threat Defense - v6.0.1 - r	Cisco ASA5555-X Threat Defe	Base, Threat, Malware, UR..	Internet Edge Perimeter

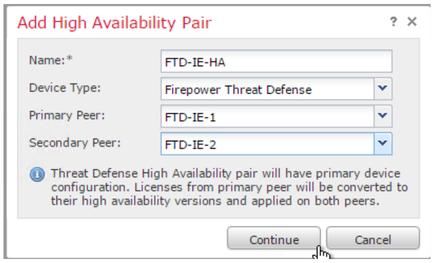
Step 4 Enter a display name for the high availability pair (e.g., FTD-IE-HA)

Step 5 For the device type, choose Firepower Threat Defense

Step 6 Select the Primary Peer device for the high availability pair

Configure FTD High Availability, continued

Step 7 Select the Secondary Peer device for the high availability pair


Add High Availability Pair

Name:* FTD-IE-HA

Device Type: Firepower Threat Defense

Primary Peer: FTD-IE-1

Secondary Peer: FTD-IE-2

Threat Defense High Availability pair will have primary device configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

Step 8 Click Continue

Step 9 Under LAN Failover Link, choose Interface G0/6 for failover communications

Step 10 Type folink for an identifying Logical Name

Step 11 Type 10.11.210.37 for the Primary IP address for the failover link on the active unit

Step 12 Type 10.11.210.38 for the Secondary IP address for the failover link on the standby unit

Step 13 Type 255.255.255.252 for the Subnet Mask of the primary and secondary IP addresses

Step 14 Under Stateful Failover Link, choose interface G0/7 for state communications

Step 15 Type statelink for an identifying Logical Name

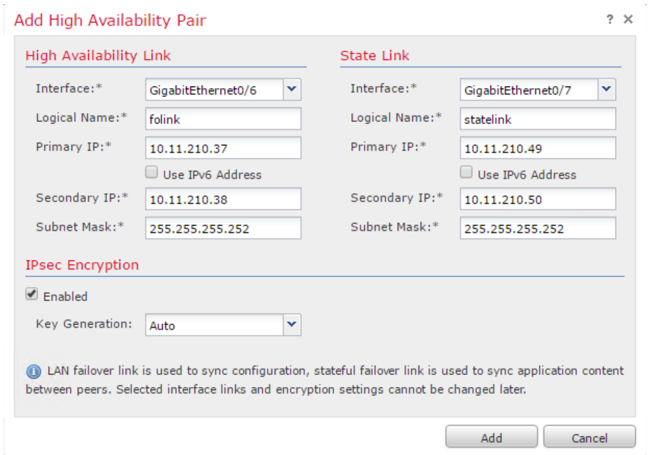
Step 16 Type 10.11.210.49 for the Primary IP address for the state link on the active unit

Step 17 Type 10.11.210.50 for the Secondary IP address for the state link on the standby unit

Step 18 Type 255.255.255.252 for the Subnet Mask of the primary and secondary IP addresses

Configure FTD High Availability, continued

Step 19 Enable Encryption on the links by choosing Enabled and select Auto for the Key Generation method for IPsec Encryption between the failover links



Add High Availability Pair

High Availability Link

Interface:*	GigabitEthernet0/6
Logical Name:*	folink
Primary IP:*	10.11.210.37
	□ Use IPv6 Address
Secondary IP:*	10.11.210.38
Subnet Mask:*	255.255.255.252

State Link

Interface:*	GigabitEthernet0/7
Logical Name:*	statelink
Primary IP:*	10.11.210.49
	□ Use IPv6 Address
Secondary IP:*	10.11.210.50
Subnet Mask:*	255.255.255.252

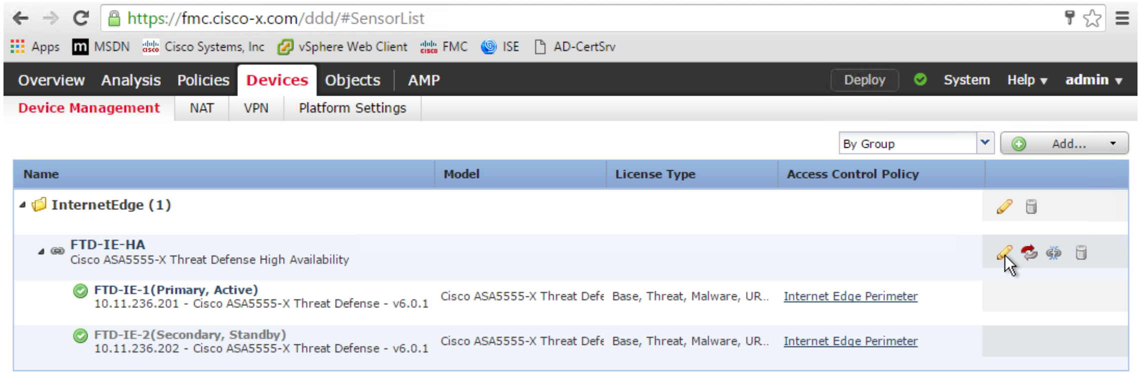
IPsec Encryption

☑ Enabled

Key Generation: Auto

LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Step 20 Click Add and wait several minutes for the systems to synchronize data. Device Management will now show the two systems beneath the High Availability group



https://fmc.cisco-x.com/ddd/#SensorList

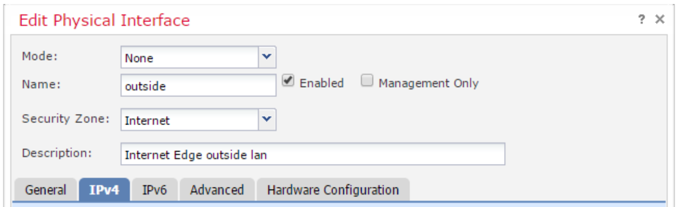
Name	Model	License Type	Access Control Policy
InternetEdge (1)			
FTD-IE-HA Cisco ASA5555-X Threat Defense High Availability			
FTD-IE-1(Primary, Active) 10.11.236.201 - Cisco ASA5555-X Threat Defense - v6.0.1	Cisco ASA5555-X Threat Defe	Base, Threat, Malware, UR...	Internet Edge Perimeter
FTD-IE-2(Secondary, Standby) 10.11.236.202 - Cisco ASA5555-X Threat Defense - v6.0.1	Cisco ASA5555-X Threat Defe	Base, Threat, Malware, UR...	Internet Edge Perimeter

Step 21 Click on the edit pencil > Interfaces to configure Inside, outside and RA VPN networks

Step 22 Click on the edit pencil for GigabitEthernet0/0

Step 23 Type outside for the name, tick the enabled box

Step 24 Select Internet for the Security Zone, add a cool descriptive name

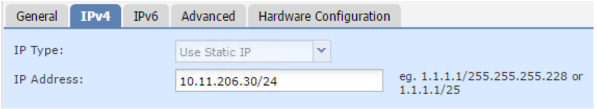


Edit Physical Interface

Mode:	None
Name:	outside ☑ Enabled □ Management Only
Security Zone:	Internet
Description:	Internet Edge outside lan

Configure FTD High Availability, continued

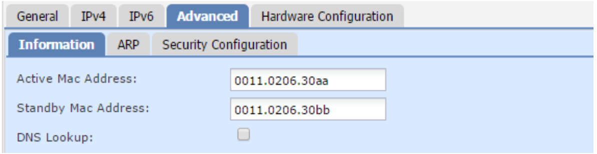
Step 25 On the IPv4 Tab, enter 10.11.206.30/24 for the IP address



IP Type: Use Static IP

IP Address: 10.11.206.30/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

Step 26 On the Advanced Tab, it is a best practice to specify the active Mac address: 0011.0206.30aa and standby Mac address: 0011.0206.30bb (these can be whatever you choose, you may base them on the IP address for simplicity)

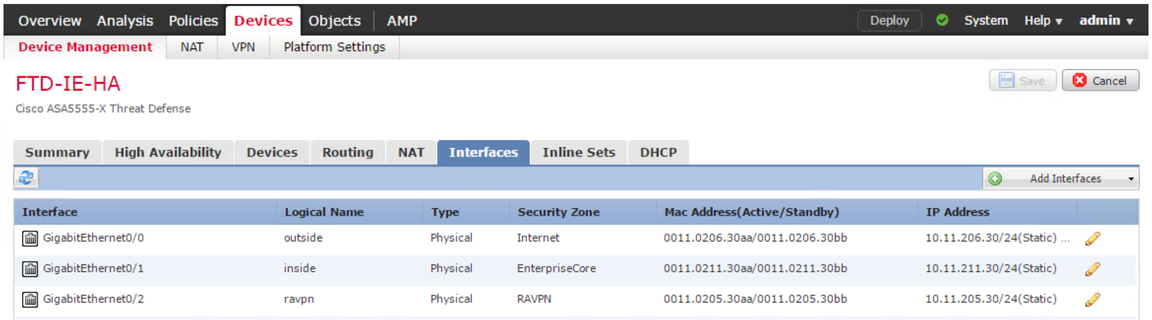


Active Mac Address: 0011.0206.30aa

Standby Mac Address: 0011.0206.30bb

DNS Lookup: □

Step 27 Click OK and repeat for the inside and RA VPN interfaces

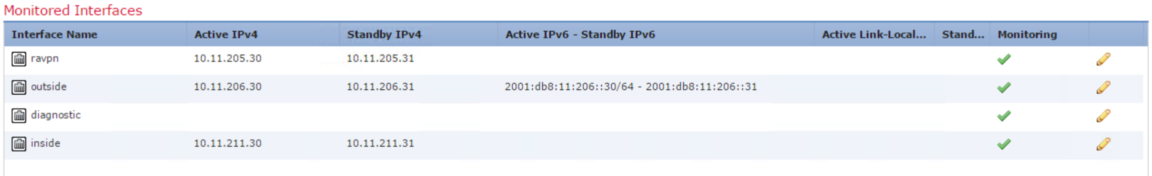


FTD-IE-HA

Cisco ASA5555-X Threat Defense

Interface	Logical Name	Type	Security Zone	Mac Address(Active/Standby)	IP Address
GigabitEthernet0/0	outside	Physical	Internet	0011.0206.30aa/0011.0206.30bb	10.11.206.30/24(Static) ...
GigabitEthernet0/1	inside	Physical	EnterpriseCore	0011.0211.30aa/0011.0211.30bb	10.11.211.30/24(Static)
GigabitEthernet0/2	ravpn	Physical	RAVPN	0011.0205.30aa/0011.0205.30bb	10.11.205.30/24(Static)

Step 28 On the High Availability Tab, edit the Monitored Interfaces and add the Standby IP address



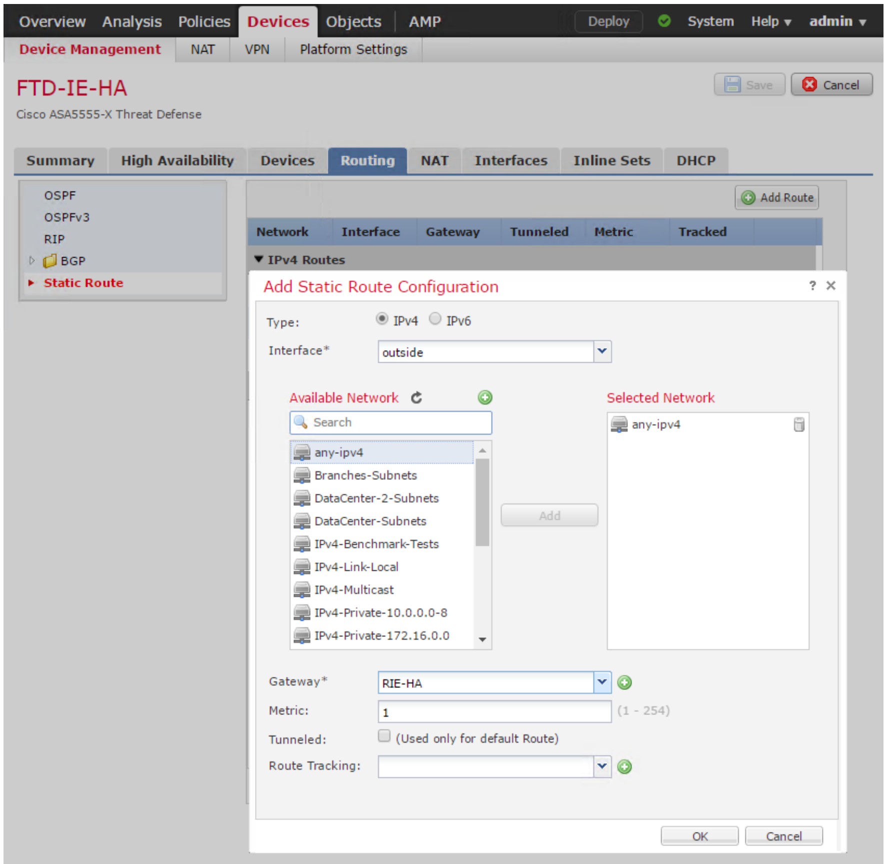
Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local...	Stand...	Monitoring
ravpn	10.11.205.30	10.11.205.31				✓
outside	10.11.206.30	10.11.206.31	2001:db8:11:206::30/64 - 2001:db8:11:206::31			✓
diagnostic						✓
inside	10.11.211.30	10.11.211.31				✓

Step 29 On the Routing Tab, select Static Route and click Add Route

Configure FTD High Availability, continued

Step 30 Select the outside interface, add the any-IPv4 network, select the gateway of the Edge routers, click OK



FTD-IE-HA

Cisco ASA5555-X Threat Defense

Add Static Route Configuration

Type: ● IPv4 ○ IPv6

Interface*: outside

Available Network: any-ipv4, Branches-Subnets, DataCenter-2-Subnets, DataCenter-Subnets, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0

Selected Network: any-ipv4

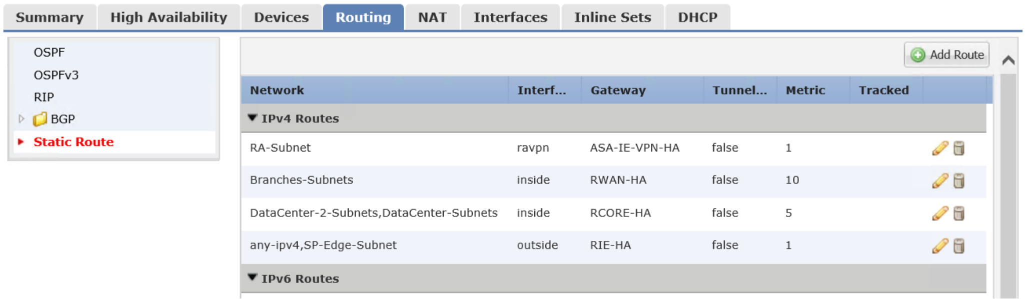
Gateway*: RIE-HA

Metric: 1 (1 - 254)

Tunneled: □ (Used only for default Route)

Route Tracking:

Step 31 Repeat for applicable inside network routes and VPN pool



Network	Interf...	Gateway	Tunnel...	Metric	Tracked
▼ IPv4 Routes					
RA-Subnet	ravpn	ASA-IE-VPN-HA	false	1	
Branches-Subnets	inside	RWAN-HA	false	10	
DataCenter-2-Subnets,DataCenter-Subnets	inside	RCORE-HA	false	5	
any-ipv4,SP-Edge-Subnet	outside	RIE-HA	false	1	
▼ IPv6 Routes					

Step 32 Click Save in the top right corner

This completes the setup of the ASA using the Firepower Threat Defense operating system. Access control policies and inspections are configured as usual.

Configure Firepower Management Center Realm

Step 1 Select System > Integration

Step 2 Select the Realms tab

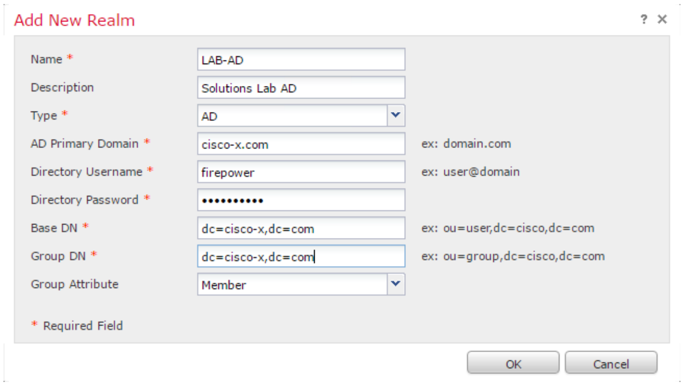
Step 3 Click New Realm on the upper right

Step 4 Type a descriptive name: LAB-AD

Step 5 Type the Primary Domain: cisco-x.com

Step 6 Type a username and password with access to the domain directory (preferably not Administrator)

Step 7 Enter the Base and Group DN: dc=cisco-x,dc=com



Add New Realm

Name *	LAB-AD	
Description	Solutions Lab AD	
Type *	AD	
AD Primary Domain *	cisco-x.com	ex: domain.com
Directory Username *	firepower	ex: user@domain
Directory Password *	••••••••••	
Base DN *	dc=cisco-x,dc=com	ex: ou=user,dc=cisco,dc=com
Group DN *	dc=cisco-x,dc=com	ex: ou=group,dc=cisco,dc=com
Group Attribute	Member	

* Required Field

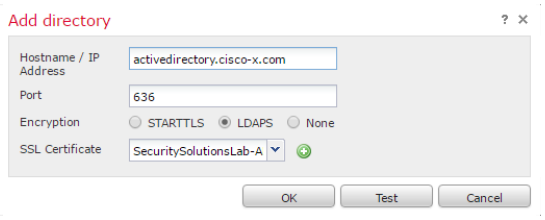
Step 8 Click OK

Step 9 Click on the newly created realm to edit it

Step 10 Click Add Directory

Step 11 Enter the hostname for the AD server: activedirectory.cisco-x.com

Step 12 Select LDAPs for a secure connection, upload and select the proper certificate



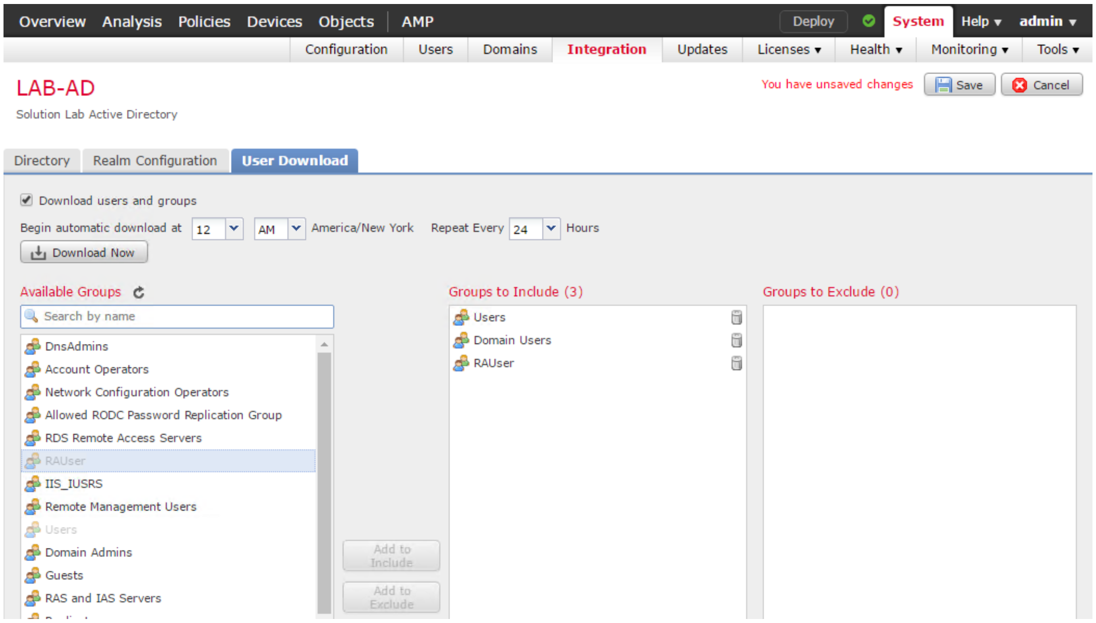
Add directory

Hostname / IP Address	activedirectory.cisco-x.com
Port	636
Encryption	○ STARTTLS ● LDAPS ○ None
SSL Certificate	SecuritySolutionsLab-A

Step 13 Click Test to verify connectivity, then OK

Configure Firepower Management Center Realm, continued

Step 14 On the User Download tab, select the groups to include/exclude



LAB-AD

Solution Lab Active Directory

☑ Download users and groups

Begin automatic download at 12 AM America/New York Repeat Every 24 Hours

Available Groups

- DnsAdmins
- Account Operators
- Network Configuration Operators
- Allowed RODC Password Replication Group
- RDS Remote Access Servers
- RAUser
- IIS_IUSRS
- Remote Management Users
- Users
- Domain Admins
- Guests
- RAS and IAS Servers

Groups to Include (3)

- Users
- Domain Users
- RAUser

Groups to Exclude (0)

Step 15 Click Save in the upper right Configure ISE Integration

Configure ISE Integration

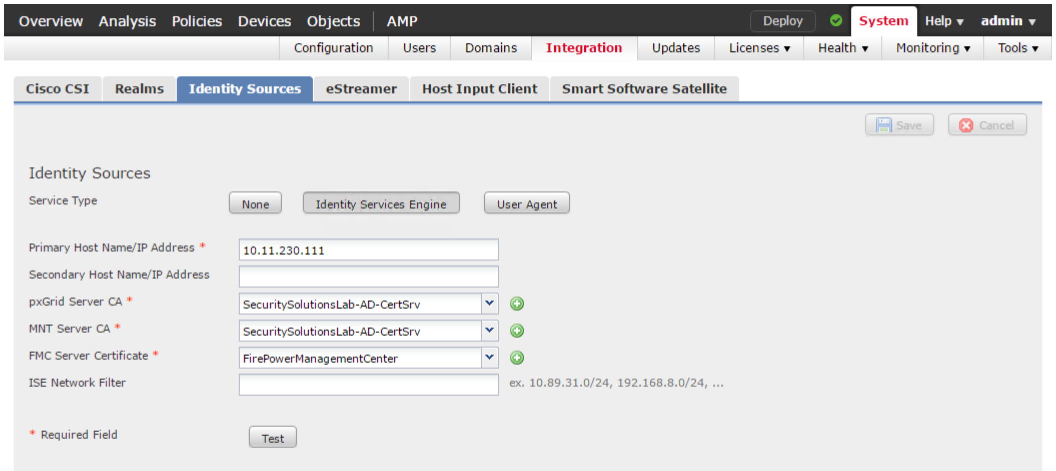
Step 1 Select System > Integration

Step 2 Select the Identity Sources tab

Step 3 Select Identity Services Engine for the Service Type to enable the ISE connection

Step 4 Type the ISE Primary Host Name/IP Address

Step 5 Select the appropriate certificate authorities from the pxGrid Server CA and MNT Server CA drop-down lists, and the appropriate certificate from the FMC Server Certificate drop-down list



Identity Sources

Service Type: None | Identity Services Engine | User Agent

Primary Host Name/IP Address *: 10.11.230.111

Secondary Host Name/IP Address:

pxGrid Server CA *: SecuritySolutionsLab-AD-CertSrv

MNT Server CA *: SecuritySolutionsLab-AD-CertSrv

FMC Server Certificate *: FirePowerManagementCenter

ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

Step 6 Click Test to verify the connection, then click Save in the upper right

For more information on integrating ISE and Firepower Management Center, please visit Cisco's Rapid Threat Containment Solution Overview: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/rapid-threat-containment/solution-overview-c22-736229.html?cachemode=refresh

How To Guide: https://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/how-to-pxgrid_sourcefire_draft_1013_je.pdf

Configure Identity Policy

Step 1 In FMC, Choose Policies > Access Control > Identity

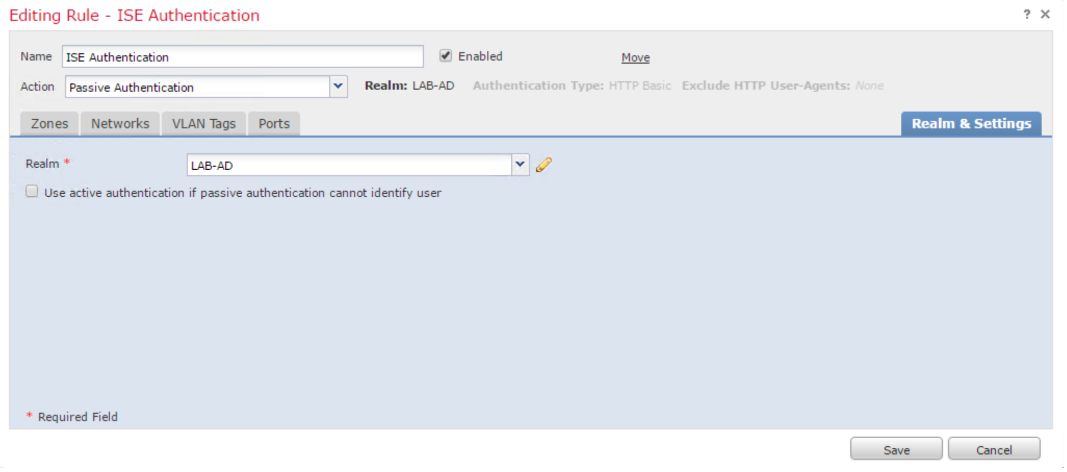
Step 2 Click Add Policy in the upper right

Step 3 Enter a descriptive name: Lab-ISE-Policy, click Save

Step 4 Click Add Rule

Step 5 Select Action: Passive Authentication

Step 6 Select Realm: Lab-AD



Editing Rule - ISE Authentication

Name: ISE Authentication ☑ Enabled

Action: Passive Authentication

Realm: LAB-AD Authentication Type: HTTP Basic Exclude HTTP User-Agents: None

Realm *: LAB-AD

☐ Use active authentication if passive authentication cannot identify user

* Required Field

Step 7 Click Save, then click Save in the upper right

Access Control Policy

The following steps outline the basic access control policy implemented in the lab for testing. Production implementation will require a more complete set of rules to fit additional use cases and acceptable risk profiles.

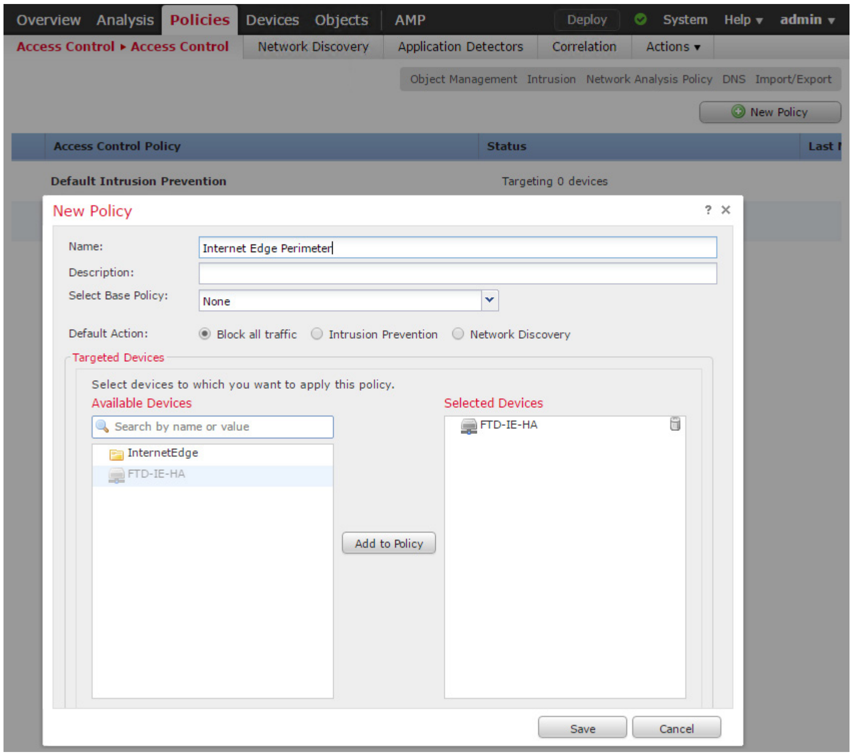
More information on Firepower Management Center Access Control policies can be found here: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Getting_Started_with_Access_Control_Policies.html

Step 1 In FMC, choose Policies > Access Control

Step 2 Click New Policy in the upper right

Step 3 Enter a display name for the Policy: Internet Edge Perimeter

Step 4 Select the FTD-IE-HA target device and click Add to Policy



Name: Internet Edge Perimeter

Description:

Select Base Policy: None

Default Action: ● Block all traffic ○ Intrusion Prevention ○ Network Discovery

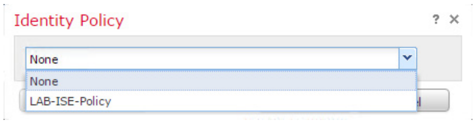
Selected Devices: FTD-IE-HA

Step 5 Click Save. Once the new policy is created, edit the policy to add rules and associate other policies.

Step 6 Click the edit pencil next to the Access Control Policy

Access Control Policy, continued

Step 7 Click Identity Policy: None, and select the appropriate Identity Policy



Identity Policy

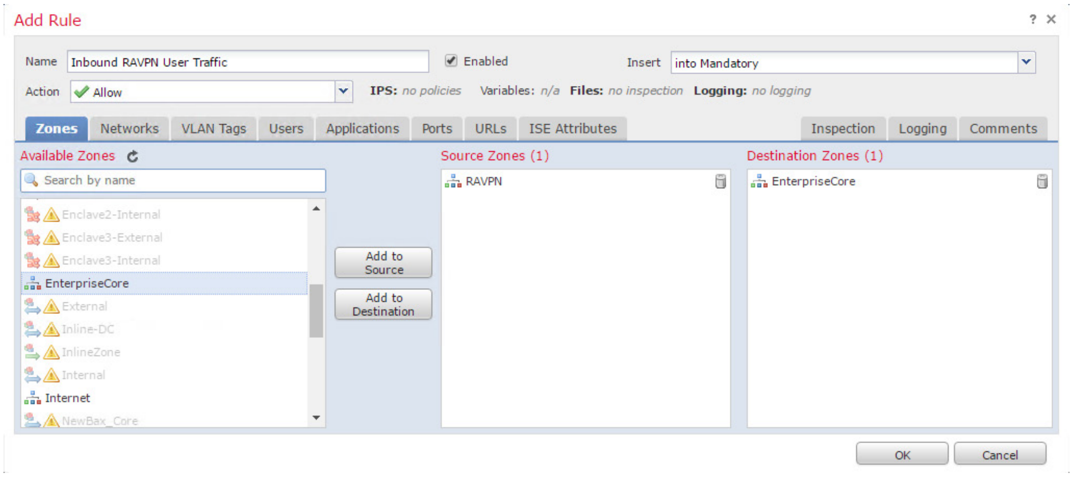
None

Step 8 Clock OK, then Save in the top right

Step 9 Click Add Rule

Step 10 Enter a display name for Rule: Inbound RA VPN User Traffic

Step 11 Assign relevant source and destination zones



Add Rule

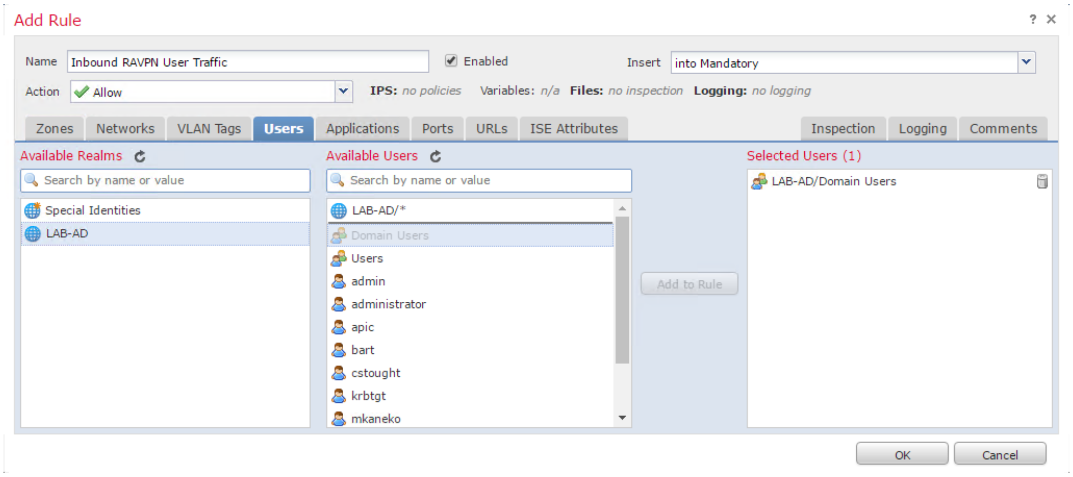
Name: Inbound RAVPN User Traffic ☑ Enabled Insert: into Mandatory

Action: ✓ Allow **IPS:** *no policies* Variables: *n/a* **Files:** *no inspection* **Logging:** *no logging*

Source Zones (1): RAVPN

Destination Zones (1): EnterpriseCore

Step 12 Assign relevant users



Add Rule

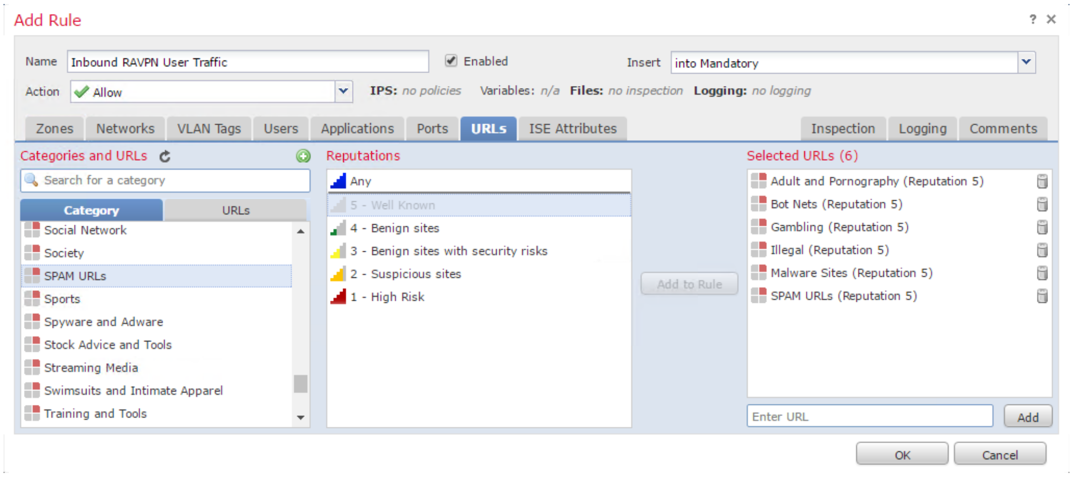
Name: Inbound RAVPN User Traffic ☑ Enabled Insert: into Mandatory

Action: ✓ Allow **IPS:** *no policies* Variables: *n/a* **Files:** *no inspection* **Logging:** *no logging*

Selected Users (1): LAB-AD/Domain Users

Access Control Policy, continued

Step 13 Block undesired URLs



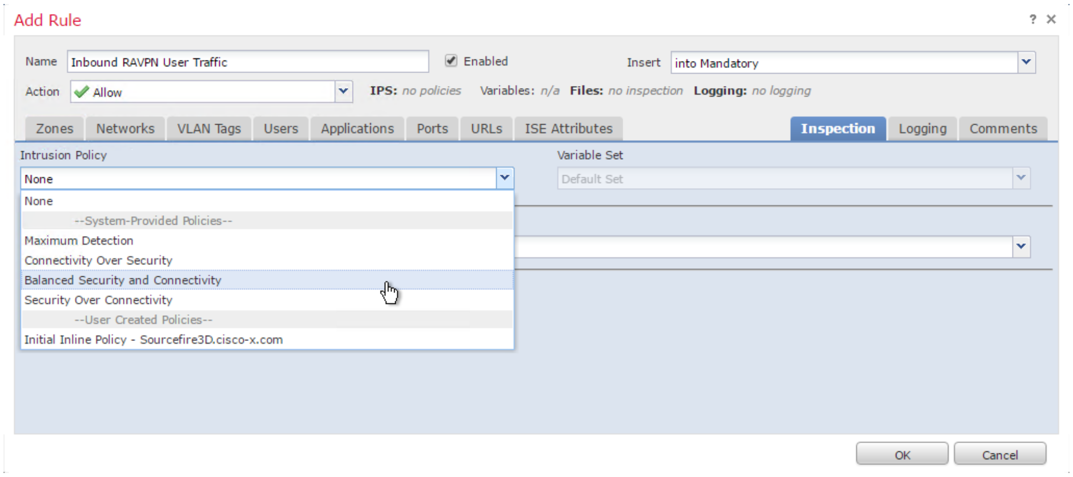
Name: Inbound RAVPN User Traffic ☑ Enabled Insert: into Mandatory

Action: ✓ Allow **IPS:** *no policies* Variables: *n/a* **Files:** *no inspection* **Logging:** *no logging*

Selected URLs (6)

- Adult and Pornography (Reputation 5)
- Bot Nets (Reputation 5)
- Gambling (Reputation 5)
- Illegal (Reputation 5)
- Malware Sites (Reputation 5)
- SPAM URLs (Reputation 5)

Step 14 Assign an appropriate Intrusion Policy


Add Rule
? ×
Zones
Networks
VLAN Tags
Users
Applications
Ports
URLs
ISE Attributes
Inspection
Logging
Comments
None
--System-Provided Policies--
Maximum Detection
Connectivity Over Security
Balanced Security and Connectivity
Security Over Connectivity
--User Created Policies--
Initial Inline Policy - Sourcefire3D.cisco-x.com
OK
Cancel

Name: Inbound RAVPN User Traffic ☑ Enabled Insert: into Mandatory

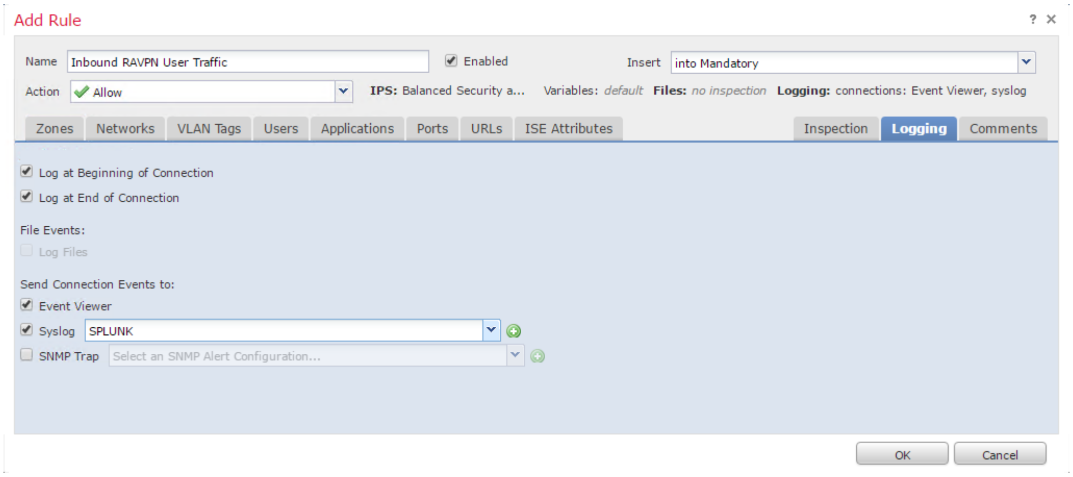
Action: ✓ Allow **IPS:** *no policies* Variables: *n/a* **Files:** *no inspection* **Logging:** *no logging*

Intrusion Policy: None

Variable Set: Default Set

Access Control Policy, continued

Step 15 Specify logging for connections



Add Rule

Name: Inbound RAVPN User Traffic ☑ Enabled Insert: into Mandatory

Action: ✓ Allow IPS: Balanced Security a... Variables: *default* Files: *no inspection* Logging: connections: Event Viewer, syslog

☑ Log at Beginning of Connection

☑ Log at End of Connection

File Events:

□ Log Files

Send Connection Events to:

☑ Event Viewer

☑ Syslog SPLUNK

□ SNMP Trap Select an SNMP Alert Configuration...

Step 16 Click OK to complete rule addition

Step 17 Click Save in the upper right

Step 18 Click Deploy at the top right to deploy the new policy and rules to the Internet FTD devices

Validation Testing

Validation included a variety of tests to verify functionality of the deployed capabilities. DDoS, AnyConnect VPN, and failover were all tested and performed satisfactorily.

Summary of Tests Performed

These tests are designed to validate the integration of and general functionality of the Remote Access VPN. The common structure of the architecture is based on the SAFE Internet Edge design.

Table 4 outlines the various tests conducted to validate the deployment.

Table 3 *Test Scenarios*

Test	Methodology
Connectivity between AnyConnect clients against Firepower 9300 running ASA code	From External, AnyConnect (PC, iOS and other platform) will create VPN session towards FP9300 running ASA code
Clientless SSL VPN validation	Set Clientless VPN using various browsers to access to the internal servers
Physical Firepower 9300 failure and recovery	In this failure scenario, Firepower 9300 manually removed and recovered power from the Master ASA device to initiate failure
FP9300 failover link failure	Fail and recover the following links: • Fail a data link to Master • Fail both data links to Master • Fail a data link to Slave • Fail both data links to Slave • Fail data link to Master
Management traffic flows	Ensure centralized management access via private VLAN and firewall access control rules
Cisco Identity Services Engine (ISE) integration	Confirm integration of the ISE with the components listed below • ISE authentication and authorization services across the infrastructure • Nexus switching • UCS domain • FP9300/ASA platforms • Directory service integration • Microsoft Active Directory Services
RadWare vDP (Virutal Defense Pro) with ASA running in FP9300	Ensure vDP will provide protection against FP9300's VPN gateway from DDoS attack

Table 4 *Summary of Results*

Test Description	Components	Result
AnyConnect connectivity to Firepower 9300 with ISE authentication	• AnyConnect • FP9300 • ISE	Successfully established SSL VPN connection using ISE as authentication server with Active directory No traffic interruption and notification syslog output was recorded
FP9300 link failure on data link	• FP9300	No traffic interruption and notification syslog output with acceptable packet loss
Radware DDoS test	• FP9300 • AnyConnect • RadWare vDP	Multiple kinds of DDoS attacks have been initiated towards gateway IP address vDP successfully identified the attacks and drop the packet to protect the VPN gateway
IPS integration	• FP9300 • ASA5555	ASA5555 running Firepower Threat Defense successfully protect network with its IPS features after the VPN traffic is decrypted by FP9300 running ASA image

Summary

Today's networks extend to wherever employees are, wherever data is, and wherever data can be accessed. The Internet edge is often the first area of attack and is subsequently the first line of defense against these attacks.

As a result, technologies must be applied that focus on detecting, understanding, and stopping threats. These attacks can render an enterprise inaccessible from the Internet and prevent employees from performing productive work locally and remotely.

Cisco's Internet edge solutions work to mitigate threats and minimize their impact on the enterprise's productivity.

References

For detailed design and configuration information for implementing a remote access VPN via Cisco AnyConnect for SSL connections, see the Remote Access VPN Technology Design Guide.

Firepower Management Center Configuration Guide, Version 6.0.1
http://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601.html

Cisco Firepower Threat Defense Quick Start Guide for the ASA
http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html

Navigating the Cisco FXOS Documentation
http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html

Cisco FXOS Firepower Chassis Manager Configuration Guide 1.1(4)
http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos114/web-config/b_GUI_ConfigGuide_FXOS_114.html

Cisco ASA Series VPN ASDM Configuration Guide, 7.6
http://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asdm76/vpn/asdm-76-vpn-config.html

Appendix

Lab Diagram

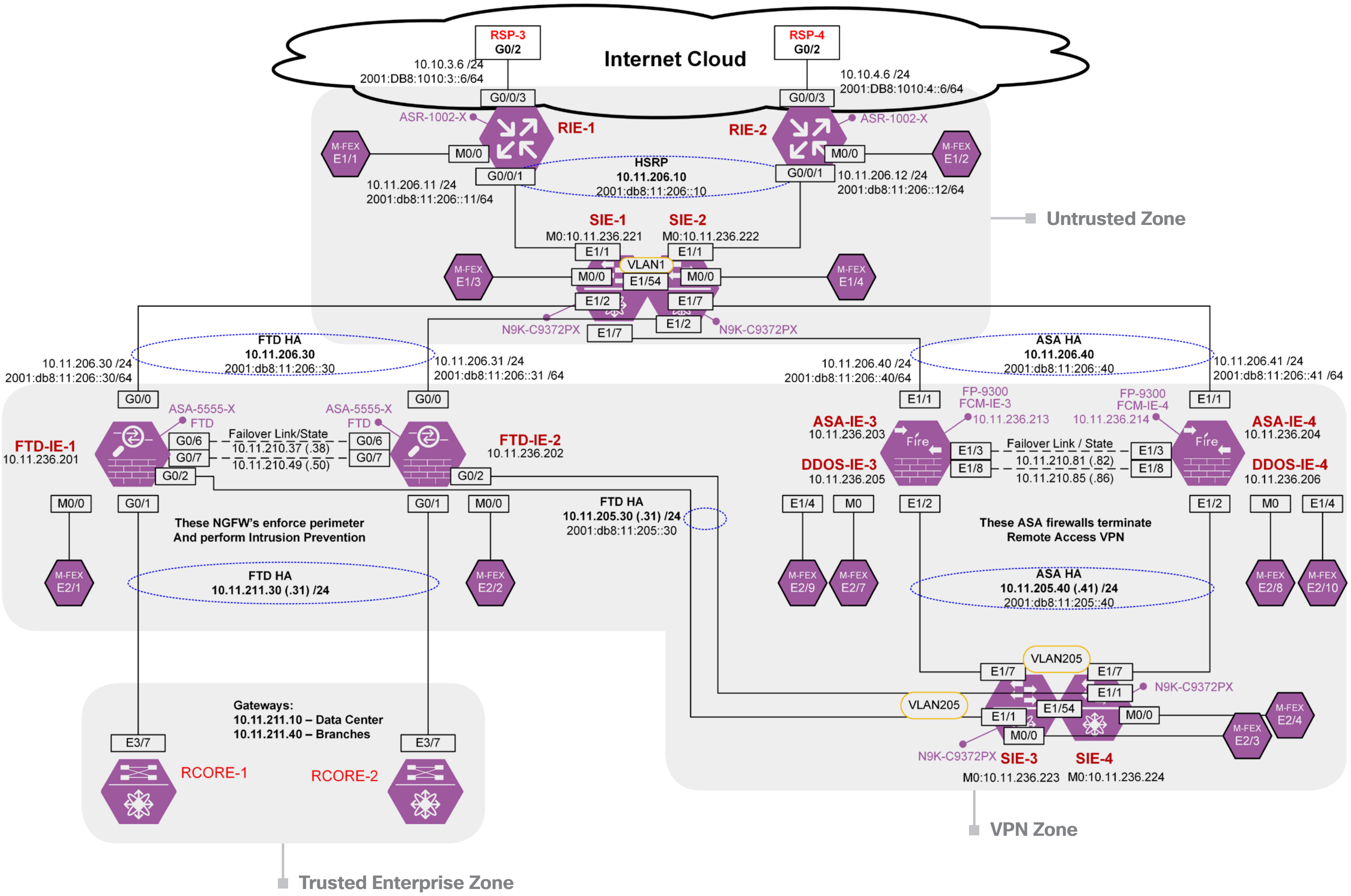


Figure 3 *Internet Edge Reference Architecture – Physical Topology*

Edge Router Configuration

```
Current configuration : 15285 bytes
!
! Last configuration change at 15:43:59 PST Fri Apr 29 2016 by bmcgloth
! NVRAM config last updated at 15:43:54 PST Fri Apr 29 2016 by bmcgloth
!
version 15.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
no platform punt-keepalive disable-kernel-core
!
hostname RIE-1
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
security authentication failure rate 2 log
security passwords min-length 7
logging buffered 50000 informational
no logging rate-limit
enable secret <removed>
!
aaa new-model
!
!
aaa group server tacacs+ PRIMARY1
 server name PRIMARY
 ip tacacs source-interface GigabitEthernet0/0/1
!
aaa authentication login COMPLIANCE group PRIMARY1 local
```

Edge Router Configuration, continued

```
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting update newinfo
aaa accounting exec default
 action-type start-stop
 group tacacs+
!
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
!
aaa accounting system default
 action-type start-stop
 group tacacs+
!
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
clock summer-time PST recurring
!
!
!
!
!


no ip bootp server
ip domain name cisco-x.com
ip name-server 10.11.230.100
!
!
!
login block-for 1800 attempts 6 within 1800
login quiet-mode access-class 23
login on-failure log
login on-success log
no ipv6 source-route
ipv6 unicast-routing
ipv6 multicast rpf use-bgp
!
!
```

Edge Router Configuration, continued

```
multilink bundle-name authenticated
password encryption aes
!
crypto pki trustpoint TP-self-signed-2651906707
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2651906707
 revocation-check none
 rsakeypair TP-self-signed-2651906707
!
!
crypto pki certificate chain TP-self-signed-2651906707
 certificate self-signed 01
  <removed>
        quit
archive
 log config
  logging enable
  notify syslog contenttype plaintext
  hidekeys
!
!
!
!
!
!
username retail privilege 15 secret 4 <removed>
username bart privilege 15 secret 4 <removed>
username emc-ncm privilege 15 secret 4 <removed>
username bmcgloth privilege 15 secret 4 <removed>
username csmadmin privilege 15 secret 4 <removed>
username ciscolms privilege 15 secret 4 <removed>
username chambers privilege 15 secret 4 <removed>
!
redundancy
 mode none
!
!
!
ip ssh version 2
ip scp server enable
!
policy-map COPPr
 class class-default
  police 8000
!
```

Edge Router Configuration, continued

```
!
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 description link to SIE-1 G1/1
 ip address 10.11.206.11 255.255.255.0
 ip access-group INTERNAL-FILTER-IN in
 standby version 2
 standby 1 ip 10.11.206.10
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication TheCure
 standby 2 ipv6 2001:DB8:11:206::10/64
 standby 2 ipv6 2001:DB8:192:22::10/64
 standby 2 priority 105
 standby 2 preempt
 standby 2 authentication TheCure
 speed 1000
 no negotiation auto
 ipv6 address 2001:DB8:11:206::11/64
 ipv6 address 2001:DB8:192:22::11/64
 ipv6 verify unicast source reachable-via rx
 ipv6 traffic-filter IPv6-INTERNAL-FILTER-IN in
!
interface GigabitEthernet0/0/2
 description link to RIE-4 G1/1
 no ip address
 shutdown
 speed 1000
 no negotiation auto
!
interface GigabitEthernet0/0/3
 description Link to RSP-3 G0/2
 ip address 10.10.3.6 255.255.255.0
 ip access-group COARSE-FILTER-INTERNET-IN in
 ip access-group COARSE-FILTER-INTERNET-OUT out
```

Edge Router Configuration, continued

```
 speed 1000
 no negotiation auto
 ipv6 address 2001:DB8:1010:3::6/64
 no ipv6 redirects
 ipv6 verify unicast source reachable-via rx allow-default
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-IN in
 ipv6 traffic-filter IPv6-COARSE-FILTER-INTERNET-OUT out
!
interface GigabitEthernet0/0/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/5
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.10.3.1
ip route 10.10.0.0 255.255.0.0 10.11.206.30
ip route 10.10.0.0 255.255.255.0 10.10.3.1
ip route 10.11.0.0 255.255.0.0 10.11.206.30
ip route 10.11.207.0 255.255.255.0 10.11.206.20
ip route 10.11.208.0 255.255.255.0 10.11.206.20
ip route 10.11.209.0 255.255.255.0 10.11.206.20
ip tacacs source-interface GigabitEthernet0/0/1
!
ip access-list extended COARSE-FILTER-INTERNET-IN
 remark ---Temporary LAB permission - remove for production networks---
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 192.168.0.0 0.0.255.255 10.0.0.0 0.255.255.255
 permit ip 172.16.0.0 0.15.255.255 10.0.0.0 0.255.255.255
 remark -------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
```

Edge Router Configuration, continued

```
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny   ip any 10.11.206.0 0.0.0.255 log
 deny   ip any 1.1.1.0 0.0.0.255 log
 remark -
 remark ---Block Spoofing of your networks---
 remark enter your IP block here
 remark ---Permit all other traffic---
 permit ip any any
ip access-list extended COARSE-FILTER-INTERNET-OUT
 remark ---Block private networks from reaching Internet---
 remark ---Temporary LAB permission - remove for production networks---
 permit ip any any
 remark -------------------------------------------------------
 remark ---Block Private Networks---
 deny   ip 10.0.0.0 0.255.255.255 any log
 deny   ip 172.16.0.0 0.15.255.255 any log
 deny   ip 192.168.0.0 0.0.255.255 any log
 remark -
 remark ---Block Autoconfiguration Networks---
 deny   ip 169.254.0.0 0.0.255.255 any log
 remark -
 remark ---Block Loopback Networks---
 deny   ip 127.0.0.0 0.0.255.255 any log
 remark -
 remark ---Block Multicast Networks---
 deny   ip 224.0.0.0 15.255.255.255 any log
 remark -
 remark ---Permit allowed protocol traffic---
 permit tcp any any
 permit udp any any
 permit icmp any any
 deny   ip any any
ip access-list extended INTERNAL-FILTER-IN
```

Edge Router Configuration, continued

```
 remark -------------------------------------------------------
 remark ---Permit Admin Management---
 permit icmp any any
 permit tcp host 10.11.230.9 host 10.11.206.11 eq 22 log
 permit tcp host 10.11.230.9 host 10.11.206.10 eq 22 log
 permit tcp host 10.11.230.111 eq tacacs host 10.11.206.11
 permit tcp host 10.11.230.111 eq tacacs host 10.11.206.10
 remark -
 remark ---Permit HSRP V2 packets---
 permit udp host 10.11.206.12 host 224.0.0.102 eq 1985
 remark -
 remark ---Deny other connections to Edge Router---
 deny   ip any host 10.11.206.11 log
 deny   ip any host 10.11.206.10 log
 deny   ip any host 10.10.3.6 log
 remark -
 remark ---Permit all other traffic to Internet---
 permit ip any any
!
logging trap informational
logging source-interface GigabitEthernet0/0/1
logging host 10.11.230.161
access-list 23 permit 10.11.230.9 log
access-list 23 deny   any log
access-list 88 permit 10.11.230.111
access-list 88 deny   any log
ipv6 route 2001:DB8:11::/48 2001:DB8:11:206::30
ipv6 route 2001:DB8:192::/48 2001:DB8:11:206::20
ipv6 route ::/0 2001:DB8:1010:3::1
!
snmp-server group V3Group v3 priv read V3Read write V3Write
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server trap-source GigabitEthernet0/0/1
snmp-server packetsize 8192
snmp-server location Building SJC-17-1 Aisle 1 Rack 1
snmp-server contact Bart McGlothin
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps entity
snmp-server enable traps hsrp
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
```

Edge Router Configuration, continued

```
snmp-server enable traps ipsla
snmp-server enable traps flash insertion removal
!
tacacs server PRIMARY
 address ipv4 10.11.230.111
 key 7 <removed>
!
!
ipv6 access-list BLOCKALL-IPv6
 deny ipv6 any any log
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-IN
 remark ---Temporary LAB permit for use of documentation IPv6 space---
 permit ipv6 2001:DB8::/32 2001:DB8::/32
 remark --------------------------------------------------------------
 remark ---Block all traffic DHCP server -> client---
 deny udp any eq 547 any eq 546
 remark ---Block all traffic DHCP client -> server---
 deny udp any eq 546 any eq 547
 remark ---Block all traffic Routing Header Type 0---
 deny ipv6 any any routing-type 0
 remark -
 remark ---Accept all ICMPv6 packets for Neighbor Discovery and Path MTU Discovery
---
 permit icmp any any nd-na
 permit icmp any any nd-ns
 permit icmp any any router-advertisement
 permit icmp any any router-solicitation
 permit icmp any any packet-too-big
 permit icmp any any destination-unreachable
 permit icmp any any unreachable
 permit icmp any any no-route
 permit icmp any any echo-reply
 permit icmp any any echo-request
 permit icmp any any time-exceeded
 permit icmp any any parameter-problem
 permit icmp any any mld-query
 permit icmp any any mld-reduction
 permit icmp any any mld-report
 permit icmp any any port-unreachable
 remark --
 remark ---Block IETF Documentation Network---
 deny ipv6 2001:DB8::/32 any
 remark ---
 remark ---Block Spoofing of Your Networks---
```

Edge Router Configuration, continued

```
 deny ipv6 2001:DB8:192::/48 any
 remark ----
 remark ---Block Traffic targeted at DMZ Network Edge Devices---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ------
 remark ---Permit Only Assigned Networks to Your Network---
 permit ipv6 2000::/3 2001:DB8:192::/48
!
ipv6 access-list IPv6-COARSE-FILTER-INTERNET-OUT
 remark ---Temporary LAB permit for use of documentation IPv6 space---
 permit ipv6 2001:DB8::/32 2001:DB8::/32
 remark -------------------------------------------------------
 remark ---Block private networks from reaching Internet---
 remark ---Block IETF reserved Networks---
 deny ipv6 FEC0::/10 any log
 deny ipv6 FC00::/7 any log
 deny ipv6 host :: any log
 deny ipv6 ::/96 any log
 deny ipv6 ::/8 any log
 deny ipv6 ::FFFF:0.0.0.0/96 any log
 deny ipv6 2001:DB8::/32 any log
 remark -
 remark ---Block Loopback Address---
 deny ipv6 host ::1 any log
 remark --
 remark ---Block Multicast Networks---
 deny ipv6 FE00::/7 any log
 remark ---
 remark ---Alternate is to Permit Traffic From My Network to Assigned Networks---
 remark ----
 permit ipv6 2001:DB8:192::/48 2000::/3
 remark -----
 remark ---Explicit Deny for All Other Networks and Log---
 deny ipv6 any any log
!
ipv6 access-list IPv6-INTERNAL-FILTER-IN
 remark -------------------------------------------------------
 permit icmp any any
 remark -
 remark ---Permit HSRP V2 packets---
 permit udp host 2001:DB8:192:22::12 eq 2029 host FF02::66 eq 2029
 permit udp host FE80::E6D3:F1FF:FE77:A202 eq 2029 host FF02::66 eq 2029
 remark ---Deny other connections to Edge Router---
 deny ipv6 any 2001:DB8:192:22::/64 log
 remark ---Permit My Network Traffic to Assigned Networks---
```

Edge Router Configuration, continued

```
 permit ipv6 2001:DB8:192::/48 2000::/3
!
control-plane
!
banner exec ^CC
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO CVD LABS ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT TO
MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY TO
IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER REPRESENTATIVES
OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT FURTHER NOTICE OR
CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER CRIMINAL CONDUCT REVEALED BY
SUCH USE IS SUBJECT TO DISCLOSURE TO LAW ENFORCEMENT OFFICIALS AND PROSECUTION TO
THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner incoming ^CC
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO CVD LABS ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT TO
MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY TO
IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER REPRESENTATIVES
OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT FURTHER NOTICE OR
CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER CRIMINAL CONDUCT REVEALED BY
SUCH USE IS SUBJECT TO DISCLOSURE TO LAW ENFORCEMENT OFFICIALS AND PROSECUTION TO
THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^C
banner login ^CCC
WARNING:
THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF AUTHORIZED USERS ONLY!


^C
!
line con 0
 session-timeout 15 output
```

Edge Router Configuration, continued

```
 exec-timeout 15 0
 login authentication COMPLIANCE
 stopbits 1
line aux 0
 session-timeout 1 output
 exec-timeout 0 1
 privilege level 0
 no exec
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 session-timeout 15 output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication COMPLIANCE
 transport preferred none
 transport input ssh
 transport output none
line vty 5 15
 session-timeout 15 output
 access-class 23 in
 exec-timeout 15 0
 ipv6 access-class BLOCKALL-IPv6 in
 logging synchronous
 login authentication COMPLIANCE
 transport preferred none
 transport input ssh
 transport output none
!
ntp authentication-key 555 md5 mysecretkey
ntp trusted-key 555
ntp authenticate
ntp source GigabitEthernet0/0/3
ntp server 171.68.10.80 prefer
ntp server 171.68.10.150
!
!
end
```

Edge Switch Configuration

```
!Command: show running-config
!Time: Sat Apr 30 17:34:37 2016

version 7.0(3)I2(2b)
hostname SIE-1
vdc SIE-1 id 1
 limit-resource vlan minimum 16 maximum 4094
 limit-resource vrf minimum 2 maximum 4096
 limit-resource port-channel minimum 0 maximum 511
 limit-resource u4route-mem minimum 248 maximum 248
 limit-resource u6route-mem minimum 96 maximum 96
 limit-resource m4route-mem minimum 58 maximum 58
 limit-resource m6route-mem minimum 8 maximum 8

feature tacacs+
feature sflow

username admin password 5 <removed> role network-admin
username bart password 5 <removed> role network-admin
username chambers password 5 <removed> role network-admin
username matt password 5 <removed> role network-admin

banner motd ^C
WARNING:
**** THIS SYSTEM IS PRIVATE PROPERTY FOR THE USE OF CISCO CVD LABS ****
**** AUTHORIZED USERS ONLY! ****

ANY USE OF THIS COMPUTER NETWORK SYSTEM SHALL BE DEEMED TO BE EXPRESS CONSENT TO
MONITORING OF SUCH USE AND TO SUCH ADDITIONAL MONITORING AS MAY BE NECESSARY TO
IDENTIFY ANY UNAUTHORIZED USER. THE SYSTEM ADMINISTRATOR OR OTHER REPRESENTATIVES
OF THE SYSTEM OWNER MAY MONITOR SYSTEM USE AT ANY TIME WITHOUT FURTHER NOTICE OR
CONSENT. UNAUTHORIZED USE OF THIS SYSTEM AND ANY OTHER CRIMINAL CONDUCT REVEALED BY
SUCH USE IS SUBJECT TO DISCLOSURE TO LAW ENFORCEMENT OFFICIALS AND PROSECUTION TO
THE FULL EXTENT OF THE LAW.

UNAUTHORIZED ACCESS IS A VIOLATION OF STATE AND FEDERAL,CIVIL AND CRIMINAL LAWS.

^

ssh key rsa 2048
ip domain-lookup
tacacs-server key 7 “fewhg123”
tacacs-server host 10.11.230.111
```

Edge Switch Configuration, continued

```
aaa group server tacacs+ CiscoISE
  server 10.11.230.111
  use-vrf management
  source-interface mgmt0
aaa group server tacacs+ tacacs
feature password encryption aes
ip access-list SwitchMgmt
 10 permit ip 10.11.230.9/32 10.11.236.221/32
 20 permit ip 10.11.236.0/24 10.11.236.221/32
copp profile strict
snmp-server user bart network-admin auth md5 ***** priv ***** localizedkey
snmp-server user matt network-admin auth md5 ***** priv ***** localizedkey
snmp-server user admin network-admin auth md5 ***** priv ***** localizedkey
snmp-server user chambers network-admin auth md5 ***** priv ***** localizedkey
rmon event 1 log trap <removed> description FATAL(1) owner PMON@FATAL
rmon event 2 log trap <removed> description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap <removed> description ERROR(3) owner PMON@ERROR
rmon event 4 log trap <removed> description WARNING(4) owner PMON@WARNING
rmon event 5 log trap <removed> description INFORMATION(5) owner PMON@INFO
ntp server 10.11.255.1 prefer use-vrf management
ntp server 10.11.255.2 use-vrf management
ntp server 172.26.129.252 use-vrf management
ntp server 172.28.189.1 use-vrf management
ntp source-interface mgmt0
aaa authentication login default group CiscoISE
aaa authentication login console group CiscoISE
aaa authorization ssh-certificate default group CiscoISE
aaa accounting default group CiscoISE
aaa authentication login error-enable

vlan 1

vrf context management
 ip domain-name cisco-x.com
 ip name-server 10.11.230.101 10.11.230.100
 ip route 0.0.0.0/0 10.11.236.1
 ip route 0.0.0.0/0 mgmt0 10.11.236.1
hardware access-list tcam region qos 0
hardware access-list tcam region vacl 256
hardware access-list tcam region racl 256
hardware access-list tcam region redirect 256
hardware access-list tcam region ns-qos 0
hardware access-list tcam region ns-vqos 0
hardware access-list tcam region ns-l3qos 0
hardware access-list tcam region rp-qos 0
```

Edge Switch Configuration, continued

```
hardware access-list tcam region rp-ipv6-qos 0
hardware access-list tcam region rp-mac-qos 0
hardware access-list tcam region sflow 256
sflow sampling-rate 50000
sflow max-sampled-size 200
sflow counter-poll-interval 100
sflow max-datagram-size 2000
sflow collector-ip 10.11.230.154 vrf management
sflow collector-port 7000
sflow agent-ip 10.11.230.154

sflow data-source interface Ethernet1/1
sflow data-source interface Ethernet1/2
sflow data-source interface Ethernet1/7


interface Ethernet1/1
  description RIE-1 port G0/0/1
  spanning-tree port type edge

interface Ethernet1/2
  description ASA-IE-1 Port G0/0
  spanning-tree port type edge

interface Ethernet1/3
  shutdown
  spanning-tree port type edge

interface Ethernet1/4
  shutdown
  spanning-tree port type edge

interface Ethernet1/5
  shutdown
  spanning-tree port type edge

interface Ethernet1/6
  shutdown
  spanning-tree port type edge

interface Ethernet1/7
  description FCM-IE-3 Port E1/1
  spanning-tree port type edge

===<Removed for Brevity>===
```

Edge Switch Configuration, continued

```
interface Ethernet1/54
  description vPC to SIE-2
  spanning-tree port type edge

interface mgmt0
  vrf member management
  ip address 10.11.236.221/24
clock timezone PST -8 0
clock summer-time PDT 2 Sun Mar 02:00 1 Sun Nov 02:00 60
cli alias name bye end exit
cli alias name wr copy run start
line console
  exec-timeout 15
line vty
  session-limit 16
  exec-timeout 15
  logout-warning 20
  access-class SwitchMgmt in
boot nxos bootflash://sup-active/nxos.7.0.3.I2.2b.bin
logging server 10.11.230.161 5 use-vrf management
logging source-interface mgmt0
```

Edge ASA configuration

```
ASA-IE-3-4# sh run
: Saved
: Serial Number: FLM195XXXXX
: Hardware:   FPR9K-SM-36, 234536 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)
:
ASA Version 9.6(0)124
!
hostname ASA-IE-3-4
enable password <removed> 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
feature strong-encryption
names
ip local pool IE-RA_AnyConnPoolNew 10.11.204.11-10.11.204.254 mask 255.255.255.0

!
interface Ethernet1/1
nameif outside
security-level 0
ip address 10.11.206.40 255.255.255.0 standby 10.11.206.41
!
interface Ethernet1/2
nameif inside
security-level 100
ip address 10.11.205.40 255.255.255.0 standby 10.11.205.41
!
interface Ethernet1/3
description LAN/STATE Failover Interface
!
interface Ethernet1/4
management-only
nameif management
security-level 0
ip address 10.11.236.203 255.255.255.0 standby 10.11.236.204
!
```

Edge ASA Configuration, continued

```
ftp mode passive
dns domain-lookup outside
dns domain-lookup inside

access-list test extended permit tcp any any
access-list permit standard permit any4
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
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 AnyConnect_Client_Local_Print extended permit udp any4 any4 eq netbios-ns
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu management 1500
failover
failover lan unit primary
failover lan interface LANFAIL Ethernet1/3
failover key *****
failover link LANFAIL Ethernet1/3
failover interface ip LANFAIL 10.10.10.1 255.255.255.0 standby 10.10.10.2
icmp unreachable rate-limit 1 burst-size 1
icmp permit any outside
asdm image disk0:/asdm.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route outside 0.0.0.0 0.0.0.0 10.11.206.10 1
route inside 10.11.0.0 255.255.0.0 10.11.205.30 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
```

Edge ASA Configuration, continued

```
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
aaa-server ISE-1 protocol radius
dynamic-authorization
aaa-server ISE-1 (inside) host 10.11.230.111
timeout 20
key *****
authentication-port 1812
accounting-port 1813
radius-common-pw *****
user-identity default-domain LOCAL
aaa authentication ssh console ISE-1
http server enable
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-
```

Edge ASA Configuration, continued

```
128-SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-
MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256
AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
crypto ca trustpoint ASDM_TrustPoint0
enrollment self
subject-name CN=ASA-IE
proxy-ldc-issuer
crl configure
crypto ca trustpool policy
crypto ikev2 policy 1
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 20
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 30
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 40
encryption des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
crypto ikev1 policy 20
authentication rsa-sig
```

Edge ASA Configuration, continued

```
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 110
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 120
authentication pre-share
encryption 3des
hash sha
group 2
```

Edge ASA Configuration, continued

```
lifetime 86400
crypto ikev1 policy 140
authentication rsa-sig
encryption des
hash sha
group 2
lifetime 86400
crypto ikev1 policy 150
authentication pre-share
encryption des
hash sha
group 2
lifetime 86400
telnet timeout 5
ssh stricthostkeycheck
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
!
tls-proxy maximum-session 1000
!
ssl cipher default fips
ssl cipher tlsv1.2 fips
ssl cipher dtlsv1 fips
ssl trust-point ASDM_TrustPoint0 outside
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.2.02075-k9.pkg 1
anyconnect image disk0:/anyconnect-macosx-i386-4.2.02075-k9.pkg 2
anyconnect image disk0:/anyconnect-linux-64-4.2.02075-k9.pkg 3
anyconnect profiles Allow_RemoteUsr disk0:/allow_remoteusr.xml
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
group-policy DfltGrpPolicy attributes
dns-server value 10.11.230.100
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
default-domain value cisco-x.com
group-policy GroupPolicy_IE-RA_AnyConnectSSL internal
group-policy GroupPolicy_IE-RA_AnyConnectSSL attributes
wins-server none
dns-server value 10.11.230.100
vpn-tunnel-protocol ikev1 ssl-client ssl-clientless
```

Edge ASA Configuration, continued

```
default-domain value cisco-x.com
webvpn
  anyconnect profiles value Allow_RemoteUsr type user
group-policy ClientlessPolicy internal
group-policy ClientlessPolicy attributes
vpn-tunnel-protocol ikev1 ssl-clientless
webvpn
  url-list value ClientLessBkMk
dynamic-access-policy-record DfltAccessPolicy
username chambers password <removed> privilege 15
tunnel-group DefaultRAGroup general-attributes
authentication-server-group ISE-1
tunnel-group DefaultWEBVPNGroup general-attributes
authentication-server-group ISE-1
tunnel-group IE-RA_AnyConnectSSL type remote-access
tunnel-group IE-RA_AnyConnectSSL general-attributes
address-pool IE-RA_AnyConnPoolNew
authentication-server-group ISE-1
authentication-server-group (inside) ISE-1
tunnel-group IE-RA_AnyConnectSSL webvpn-attributes
group-alias IE-RA_AnyConnectSSL enable
tunnel-group IE-RA_ClientLess type remote-access
tunnel-group IE-RA_ClientLess general-attributes
default-group-policy ClientlessPolicy
!
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 ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
```

Edge ASA Configuration, continued

```
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect dns preset_dns_map
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
no call-home reporting anonymous
call-home
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 18
  subscribe-to-alert-group configuration periodic monthly 18
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:4d1cbe6a293750053102f56159983e05
: end
```

For more information on SAFE, see www.cisco.com/go/SAFE.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**