Migrating from the Cisco ASA 5500 to the Cisco Adaptive Security Virtual Appliance

April 24, 2014

Contents

Overview

Although the ASAv shares a common software foundation with the Cisco ASA 5500, you cannot directly use an ASA 5500 configuration on an ASAv. You must modify the ASA 5500 configuration and remove configurations for all features that are not supported on the ASAv.

Supported Platforms for Migration

You may migrate all ASA hardware devices that have 8.4(x) and later software installed on them.

Cisco Systems, Inc.
www.cisco.com

Unsupported Features

The ASAv does not support the following ASA features:

- Clustering
- Multiple context mode
- Active/Active failover
- EtherChannels
- Advanced Inspection and Prevention Security Services Module (AIP SSM)
- Content Security and Control Security Services Module (CSC SSM)
- Context Security (CX) Module
- Shared AnyConnect Premium Licenses

Modifying a Cisco ASA 5500 Configuration to an ASAv Configuration

To migrate an ASA 5500 configuration to an ASAv configuration, follow these guidelines:

Guidelines

- You may perform a migration using either the CLI or ASDM.
- To use ASDM, you must configure the ASAv for HTTP access.
- Use a text editor to modify the source configuration file for the ASAv.
- The ASAv does not support multiple context mode; you can, however, convert a security context configuration into an ASAv configuration.
- The ASAv does not support ASA clustering; therefore, the cluster-related interface configuration needs to be removed before you can use it on the ASAv.

Note You may copy an unmodified hardware configuration onto an ASAv. However, you will receive "Invalid Input" and other errors or warnings for the commands that are not supported in this version of the virtual platform.

Detailed Steps

The following table lists the steps that are required to change an ASA 5500 configuration to an ASAv configuration.

Step	Task Description	Reference
1.	To upgrade an ASA 5500 configuration to Version 9.2(1), you can leverage a built-in ASAv migration tool. This tool activates when you reboot if the startup configuration matches older ASA versions. Version 9.2(1) then migrates feature-related commands that have changed from the version that was originally stored in the startup configuration.	See the ASA release notes for more information about configuration migration and for upgrade guidelines.
2.	Retrieve the ASA 5500 firewall configuration file from the source device, and store it on your local file system.	See the "Managing Software and Configurations" chapter in the General Operations CLI Configuration Guide.
3.	Choose one of the following two options: **Using the CLI** Export the following VPN configuration files: • Any clientless secure socket layer (SSL) customizations or plugins. • Any AnyConnect, Cisco Secure Desktop, and host scan images from the ASA 5500. • The PKCS12 file for the identity certificate from the ASA 5500. **Note** Make sure that you place the files in the same path that is specified in the configuration.	See the "Clientless SSL VPN Overview" chapter in the VPN CLI Configuration Guide. See the "Configuring AnyConnect VPN Client Connections" chapter in the VPN CLI Configuration Guide. See the "Installing and Enabling CSD" chapter in the Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators. See the "Configuring AnyConnect Host Scan" chapter in the VPN CLI Configuration Guide. See the "Configuring Digital Certificates" chapter in the General Operations CLI Configuration Guide. See the "Configuring Policy Groups" chapter in the VPN CLI Configuration Guide.
	Using ASDM We encourage you to use the ASDM Backup Utility to facilitate this process and save the source files. These VPN-specific files may include the following: all security images, identity certificates, VPN pre-shared keys, and all SSL VPN configurations. **Note** Make sure that you uncheck the running and startup configuration check boxes to exclude them from the backup process.	See the "Managing Software and Configurations" chapter in the General Operations ASDM Configuration Guide.
4.	Change the ASA 5500 configuration to an ASAv configuration:	—
a.	Change any interface configuration to match the available interfaces on the ASAv: Management 0/0 and GigabitEthernet 0/0 - 0/8 (for a ten-interface deployment). Remove EtherChannel interfaces.	See the "Starting Interface Configuration (ASA 5510 and Higher)" chapter in the General Operations CLI Configuration Guide.
b.	Remove the Content Security and Control Security Services Module configuration (if one is installed).	See the "Configuring the ASA CSC Module" chapter in the Firewall CLI Configuration Guide.

Step	Task Description	Reference
c.	Remove the Advanced Inspection and Prevention Security Services Module configuration (if one is installed).	See the "Configuring the ASA IPS Module" chapter in the Firewall CLI Configuration Guide.
d.	Remove the CX module configuration (if one is installed).	See the "Configuring the ASA CX Module" chapter in the Firewall CLI Configuration Guide.
e.	Remove the following unsupported features: • Multiple context mode • Clustering—Remove the **cluster-pool** and **mgmt-pool** keywords and arguments from the **ip address** command. • Active/Active Failover	See the "Configuring Multiple Context Mode" chapter in the General Operations CLI Configuration Guide. See the "Configuring a Cluster of ASAs" chapter in the General Operations CLI Configuration Guide. See the "Configuring Failover" chapter in the General Operations CLI Configuration Guide.
5.	Deploy the ASAv. To enable ASDM connectivity, you need to set appropriate properties, including the mapping of interfaces, in the OVF template. Install the ASAv onto a VM using the VMware vSphere client.	See the "Deploying the Cisco Adaptive Security Virtual Appliance" chapter in the Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide.
6.	Connect to the ASAv and configure SSH or Telnet for basic connectivity. From the CLI, use the **telnet, ssh**, or **http** command. In ASDM, choose **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**.	See the "Deploying the Cisco Adaptive Security Virtual Appliance" chapter in the Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide.
7.	Find your ASAv serial number, then you can obtain a new license that is required to run the ASAv in standard mode. From the CLI, enter the **show version** or **show inventory** command. In ASDM, choose **Help > About the Cisco ASA**. You must also request additional feature licenses that match to what is configured on your ASA hardware.	See the "Deploying the Cisco Adaptive Security Virtual Appliance" chapter in the Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide.
8.	Import the VPN-specific files that you obtained from performing Step 3. If you obtained an ASDM backup zip file, you can then restore it onto the ASAv. In ASDM, choose **Tools > Restore Configurations**. **Note** If you issue the **anyconnect-essentials** command or the **no anyconnect-essentials** command, the following message appears: `"ERROR: Command required AnyConnect Essentials license"`	See the "Clientless SSL VPN Overview" chapter in the VPN CLI Configuration Guide. See the "Configuring AnyConnect VPN Client Connections" chapter in the VPN CLI Configuration Guide. See the "Installing and Enabling CSD" chapter in the Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators.

Step	Task Description	Reference
9.	Copy the modified ASA 5500 configuration into the ASAv startup configuration. Then enter the **reload noconfirm** command to reload the ASAv and preserve the copied startup configuration. You can only use copy-and-paste or read-from-file methods on files that have been saved with Version 9.2(1) and modified in previous steps. These methods may leave interfaces in a shut-down state, may conflict with running configurations, and will not trigger the ASA migration tool. The VMware vSphere client console window does not allow you to copy and paste information. You must use a TFTP, HTTP, or FTP server to transfer the modified configuration file by entering either the **configure net** or **copy running-config** command from the CLI.	See the "Configuring Management Access" chapter in the General Operations CLI Configuration Guide. See the **reload noconfirm** command in the Command Reference. See the "Configuring Digital Certificates" chapter in the General Operations CLI Configuration Guide. See the **configure net** or **copy running-config** command in the Command Reference.
10.	Verify the modified configuration on the ASAv:	—
a.	From the CLI, use the **show startup-config errors** command to view any errors that the ASAv detected as it booted. In ASDM, choose **Tools > Command Line Interface**.	See the **show startup-config errors** command in the Command Reference. See the "Managing Software and Configurations" chapter in the General Operations ASDM Configuration Guide.
b.	Review the configuration for interfaces that may be disabled, but should not be. From the CLI, enter the **no shutdown** command. In ASDM, choose **Configuration > Device Management > Interfaces**.	See the **no shutdown** command in the Command Reference. See the "Completing Interface Configuration (Routed Mode)" chapter in the General Operations ASDM Configuration Guide.
c.	Verify that the access lists, interfaces, and inspections are correct. In the CLI, use the **show running-config** command to confirm that the ASAv configuration is correct. In ASDM, choose **Tools > Command Line Interface**.	See the "Using the ACL Manager" chapter in the General Operations ASDM Configuration Guide. See the "Starting Interface Configuration (ASA 5510 and Higher)" chapter in the General Operations ASDM Configuration Guide. See the "Getting Started with Application Layer Protocol Inspection" chapter in the Firewall ASDM Configuration Guide. See the **show running-config** command in the Command Reference.
d.	Test the modified configuration on the ASAv for the desired behavior before deploying it in production. From the CLI, use the **packet-tracer** command. In ASDM, choose **Tools > Packet Tracer**.	See the **packet tracer** command in the Command Reference. See the "Troubleshooting" chapter in the General Operations ASDM Configuration Guide.

Sample Configuration Files

Basic Configuration Before Migration

The following is a basic sample configuration file from an ASA 5525-X before migration to the ASAv:

```
Admin context:

: Saved
:
ASA Version 9.1(3) <context>
!
hostname admin
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool outside_pool 10.1.2.2-10.1.2.10 mask 255.255.255.0
ip local pool inside_pool 10.1.1.2-10.1.1.10 mask 255.255.255.0
ip local pool mgmt-pool 172.16.1.241-172.16.1.245
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 172.16.1.240 255.255.255.0
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.1.2.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
same-security-traffic permit inter-interface
access-list global extended permit icmp any any
access-list global extended permit ip any any
pager lines 24
logging console warnings
logging buffered debugging
logging asdm informational
mtu mgmt 1500
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
no asdm history enable
arp timeout 14400
access-group global in interface inside
access-group global in interface outside
access-group global global
!
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
 timers spf 1 1
```

```
 timers lsa-group-pacing 1
 log-adj-changes
!
route outside 0.0.0.0 0.0.0.0 10.1.2.200 200
route inside 10.10.140.0 255.255.255.0 10.1.1.200 200
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 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
http server enable
http 0.0.0.0 0.0.0.0 mgmt
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
no threat-detection statistics tcp-intercept
!
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 dns preset_dns_map
  inspect ftp
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
Cryptochecksum:0e8178ab18e3d553aabeee98f2192418
: end
```

Basic Configuration After Migration

The following is a basic sample configuration file from an ASA 5525-X after migration to the ASAv:

```
admin# show running-config
hostname admin
enable password 2KFQnbNIdI.2KYOU 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
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool outside_pool 10.1.2.2-10.1.2.10 mask 255.255.255.0
ip local pool inside_pool 10.1.1.2-10.1.1.10 mask 255.255.255.0
!
interface GigabitEthernet0/0
 shutdown
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
interface GigabitEthernet0/1
 shutdown
 nameif outside
 security-level 0
 ip address 10.1.2.1 255.255.255.0
 ospf hello-interval 1
 ospf dead-interval 2
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/8
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 172.16.1.240 255.255.255.0
!
ftp mode passive
same-security-traffic permit inter-interface
access-list global extended permit icmp any any
access-list global extended permit ip any any
pager lines 24
logging console warnings
logging buffered debugging
logging asdm informational
mtu mgmt 1500
mtu inside 1500
mtu outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group global in interface inside
access-group global in interface outside
access-group global global
router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 network 10.1.2.0 255.255.255.0 area 0
 log-adj-changes
!
route outside 0.0.0.0 0.0.0.0 10.1.2.200 200
route inside 10.10.140.0 255.255.255.0 10.1.1.200 200
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 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
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 0.0.0.0 0.0.0.0 mgmt
no snmp-server location
no snmp-server contact
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect dns preset_dns_map
  inspect icmp
!
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 8
  subscribe-to-alert-group configuration periodic monthly 8
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:ab49a0b37aa11997ffb6cadaaf2c5fe4
: end
admin#
```

Configuration with VPN Before Migration

Before migration, make sure that the following two requirements have been met:

- Pre-shared keys with ***** have an actual key.
- The vCPU and AnyConnect Essentials feature licenses have been added.

The following is a sample configuration file with VPN from an ASA 5515-X before migration to the ASAv:

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.2(0)3
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU 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
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RASSLVPN 10.20.20.101-10.20.20.110 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 10.30.30.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 10.20.20.2 255.255.255.0
 no shutdown
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.0.0.152 255.255.0.0
```

```
!
ftp mode passive
dns domain-lookup management
dns domain-lookup Outside
dns domain-lookup Inside
access-list ACL-OUTSIDE extended permit icmp any any
access-list Inside_cryptomap extended permit ip 10.30.30.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list bla extended permit ip any any
access-list block extended deny ip any any
pager lines 23
logging enable
logging console debugging
logging asdm informational
mtu management 1500
mtu Outside 1500
mtu Inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group block in interface Outside
route management 0.0.0.0 0.0.0.0 10.0.0.1 200
route Inside 10.10.0.0 255.255.0.0 10.20.20.1 1
route Inside 192.168.0.0 255.255.0.0 10.20.20.1 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 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
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.0.0.0 255.255.0.0 management
http 0.0.0.0 0.0.0.0 Outside
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes 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-SHA esp-aes-192 esp-sha-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-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
```

```
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map Inside_map 1 match address Inside_cryptomap
crypto map Inside_map 1 set peer 10.20.20.1
crypto map Inside_map 1 set ikev1 transform-set ESP-AES-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 map Inside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map Inside_map interface Inside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 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 enable Inside
```

```
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 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 40
 authentication crack
 encryption aes-192
 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 70
 authentication crack
 encryption aes
 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 100
 authentication crack
 encryption 3des
 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
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 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 0.0.0.0 0.0.0.0 management
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable Outside
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 internal-password enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
 webvpn
  url-list value Bookmark
group-policy "GroupPolicy_AnyConnect RA SSL VPN" internal
group-policy "GroupPolicy_AnyConnect RA SSL VPN" attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
group-policy GroupPolicy_10.20.20.1 internal
group-policy GroupPolicy_10.20.20.1 attributes
 vpn-tunnel-protocol ikev2
username admin password 2KFQnbNIdI.2KYOU encrypted privilege 15
tunnel-group "AnyConnect RA SSL VPN" type remote-access
tunnel-group "AnyConnect RA SSL VPN" general-attributes
 address-pool RASSLVPN
 default-group-policy "GroupPolicy_AnyConnect RA SSL VPN"
tunnel-group "AnyConnect RA SSL VPN" webvpn-attributes
 group-alias "AnyConnect RA SSL VPN" enable
```

```
tunnel-group 10.20.20.1 type ipsec-l2l
tunnel-group 10.20.20.1 general-attributes
 default-group-policy GroupPolicy_10.20.20.1
tunnel-group 10.20.20.1 ipsec-attributes
 ikev1 pre-shared-key Cisco1
 ikev2 remote-authentication pre-shared-key Cisco2
 ikev2 local-authentication pre-shared-key Cisco3
tunnel-group ClientlessVPN type remote-access
tunnel-group ClientlessVPN webvpn-attributes
 group-alias ClientlessVPN 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
 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 2
  subscribe-to-alert-group configuration periodic monthly 2
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:7359004446ef826e734dc5413e1c669d
: end
ciscoasa#
```

Configuration with VPN After Migration

The following is a sample configuration file with VPN from an ASA 5515-X after migration to the ASAv:

```
ciscoasa# show running-config
: Saved
:
```

```
ASA Version 9.2(0)3
!
hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU 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
passwd 2KFQnbNIdI.2KYOU encrypted
names
ip local pool RASSLVPN 10.20.20.101-10.20.20.110 mask 255.255.255.0
!
interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 10.30.30.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 10.20.20.2 255.255.255.0
!
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
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/7
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/8
 shutdown
```

```
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.0.0.152 255.255.0.0
!
ftp mode passive
dns domain-lookup management
dns domain-lookup Outside
dns domain-lookup Inside
access-list ACL-OUTSIDE extended permit icmp any any
access-list Inside_cryptomap extended permit ip 10.30.30.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list bla extended permit ip any any
access-list block extended deny ip any any
pager lines 23
logging enable
logging console debugging
logging asdm informational
mtu management 1500
mtu Outside 1500
mtu Inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group block in interface Outside
route management 0.0.0.0 0.0.0.0 10.0.0.1 200
route Inside 10.10.0.0 255.255.0.0 10.20.20.1 1
route Inside 192.168.0.0 255.255.0.0 10.20.20.1 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 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
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.0.0.0 255.255.0.0 management
http 0.0.0.0 0.0.0.0 Outside
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes 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-SHA esp-aes-192 esp-sha-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-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
```

```
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 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 map Inside_map 1 match address Inside_cryptomap
crypto map Inside_map 1 set peer 10.20.20.1
crypto map Inside_map 1 set ikev1 transform-set ESP-AES-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 map Inside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map Inside_map interface Inside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 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 enable Inside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 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 40
 authentication crack
 encryption aes-192
 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 70
 authentication crack
 encryption aes
 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 100
```

```
 authentication crack
 encryption 3des
 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
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 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 0.0.0.0 0.0.0.0 management
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
 enable Outside
 no anyconnect-essentials
 anyconnect enable
 tunnel-group-list enable
 internal-password enable
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
group-policy "GroupPolicy_AnyConnect RA SSL VPN" internal
group-policy "GroupPolicy_AnyConnect RA SSL VPN" attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ssl-client
 default-domain none
group-policy GroupPolicy_10.20.20.1 internal
group-policy GroupPolicy_10.20.20.1 attributes
 vpn-tunnel-protocol ikev2
username admin password 2KFQnbNIdI.2KYOU encrypted privilege 15
```

```
tunnel-group "AnyConnect RA SSL VPN" type remote-access
tunnel-group "AnyConnect RA SSL VPN" general-attributes
 address-pool RASSLVPN
 default-group-policy "GroupPolicy_AnyConnect RA SSL VPN"
tunnel-group "AnyConnect RA SSL VPN" webvpn-attributes
 group-alias "AnyConnect RA SSL VPN" enable
tunnel-group 10.20.20.1 type ipsec-l2l
tunnel-group 10.20.20.1 general-attributes
 default-group-policy GroupPolicy_10.20.20.1
tunnel-group 10.20.20.1 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
tunnel-group ClientlessVPN type remote-access
tunnel-group ClientlessVPN webvpn-attributes
 group-alias ClientlessVPN 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 dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
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 2
  subscribe-to-alert-group configuration periodic monthly 2
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:96fc251e97bea6a4223f8f3d2de3ae15
: end
ciscoasa# %ASA-7-111009: User 'enable_15' executed cmd: show running-config
```

Related Documentation

For additional information about the ASA 5500 and the ASAv, go to:

http://www.cisco.com/go/asadocs

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.