ASA: Multi-Context Mode Remote-Access (AnyConnect) VPN

Introduction

This document describes how to configure Remote Access (RA) Virtual Private Network (VPN) on Cisco Adaptive Security Appliance (ASA) firewall in Multiple Context (MC) mode using the CLI. It shows the Cisco ASA in multiple context mode supported/unsupported features and licensing requirement with respect to RA VPN.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ASA AnyConnect SSL Configuration
- ASA Multiple Context Configuration

Components Used

The information in this document is based on these software and hardware versions:

- AnyConnect Secure Mobility Client version 4.4.00243
- Two ASA5525 with ASA Software Version 9.6(2)

> **Note**: Download the AnyConnect VPN Client package from the Cisco Software Download (registered customers only) .

> **Note**: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Multi-context is a form of virtualization that allows multiple independent copies of an application to run simultaneously on the same hardware, with each copy (or virtual device) appearing as a separate physical device to the user. This allows a single ASA to appear as multiple ASAs to multiple independent users. The ASA family has supported virtual firewalls since its initial release; however, there was no virtualization support for Remote Access in the ASA. VPN LAN2LAN (L2L) support for multi-context was added for the 9.0 release.

> **Note**: From **9.5.2** multi-context based virtualization support for VPN Remote Access (RA)

connections to the ASA.

From **9.6.2** we have support for Flash Virtulaization which means we can have Anyconnect image per context.

Feature History for Multicontext

New Features added in ASA 9.6(2)

Feature	Description
Pre-fill/Username-from-cert feature for multiple context mode	AnyConnect SSL support is extended, allowing pre-fill/username-from-certificate feature CLIs, previously available only in single mode, to be enabled in multiple context mode as well.
Flash Virtualization for Remote Access VPN	Remote access VPN in multiple context mode now supports flash virtualization. Each context can have a private storage space and a shared storage place based on the total flash that is available.
AnyConnect client profiles supported in multi-context devices	AnyConnect client profiles are supported in multi-context devices. To add a new profile using ASDM, you must have the AnyConnect Secure Mobility Client release 4.2.00748 or 4.3.03013 and later.
Stateful failover for AnyConnect connections in multiple context mode	Stateful failover is now supported for AnyConnect connections in multiple context mode.
Remote Access VPN Dynamic Access Policy (DAP) is supported in multiple context mode	You can now configure DAP per context in multiple context mode.
Remote Access VPN CoA (Change of Authorization) is supported in multiple context mode	You can now configure CoA per context in multiple context mode.
Remote Access VPN localization is supported in multiple context mode	Localization is supported globally. There is only one set of localization files that are shared across different contexts.
Packet capture storage per context is supported.	The purpose of this feature is to allow user to copy a capture directly from a context to the external storage or to the context private storage on flash. This feature also enables to copy the raw capture to the external packet capture tools such as wire-shark from within a context.

Features in ASA 9.5(2)

Feature	Description
AnyConnect 4.x and later (SSL VPN only; no IKEv2 support)	Multi-context based virtualization support for VPN Remote Access (RA) connec to the ASA.
Centralized AnyConnect image configuration	• Flash storage are not virtualized. • AnyConnect image is configured globally in the admin context and the

	configuration applies to all contexts
AnyConnect image upgrade	AnyConnect client profiles are supported in multi-context devices. To add a ne profile using ASDM, you must have the AnyConnect Secure Mobility Client rele 4.2.00748 or 4.3.03013 and later.
Context Resource Management for AnyConnect connections	• Configurability to control maximum license usage per context • Configurability to allow license bursting per context

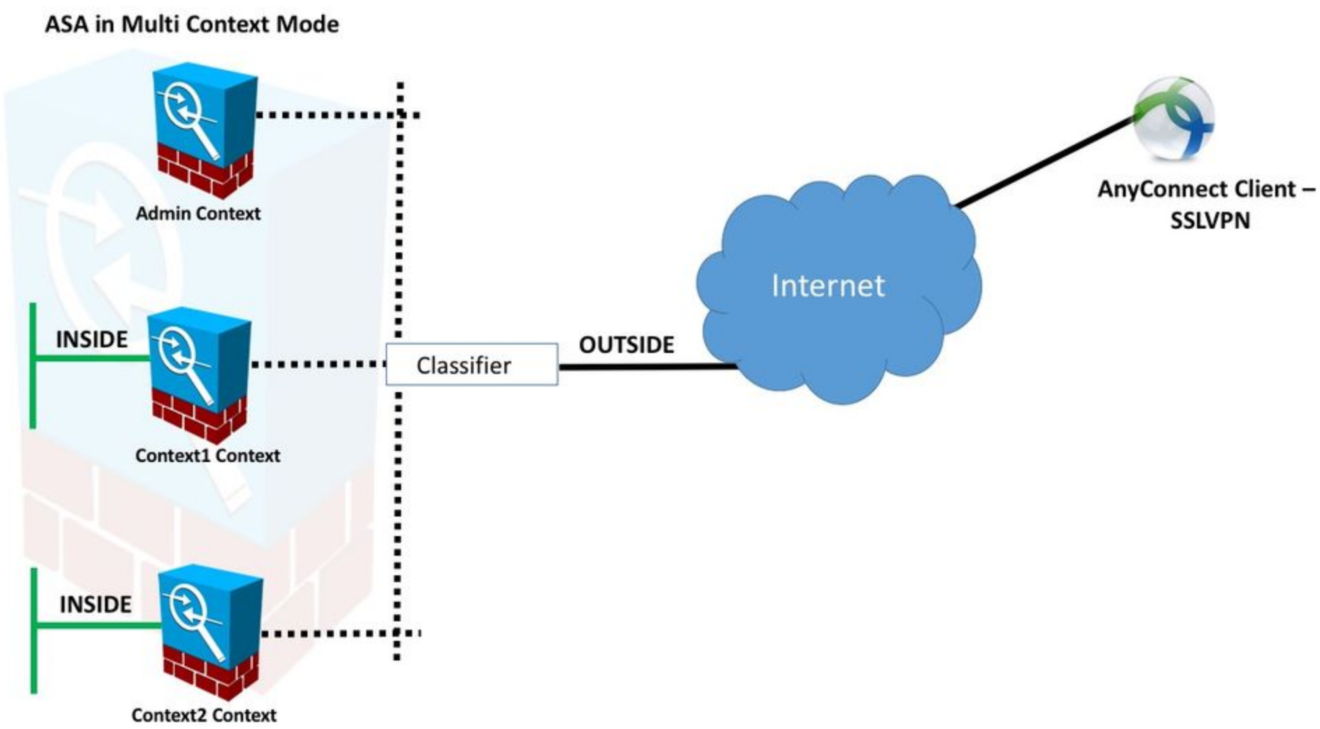
Licensing

- AnyConnect Apex license required
- Essentials licenses ignored/not allowed
- Configurability to control maximum license usage per context
- Configurability to allow license bursting per context

Configure

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram



Note: Multiple contexts in this example shares an interface (OUTSIDE), then the classifier uses the interface unique (auto or manual) MAC addresses to forward packets. For more details on how security appliance classifies packets in multiple context refer How the ASA Classifies Packets

The following configuration procedure is with ASA 9.6.2 version and above, which illustrates some of the new features available.The differences in the configuration procedure for ASA versions before 9.6.2 (and above 9.5.2) are documented in the Appendix A of the document.

The necessary configurations in System Context and Custom Contexts for setting up Remote Access VPN are described below:

Initial configurations in System Context

To begin with, in System Context configure failover, VPN resource allocation, custom contexts and Apex license verification. The procedure and configurations are described in this section, and in the next section

Step 1. Failover Configuration.

```
 !! Active Firewall

failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

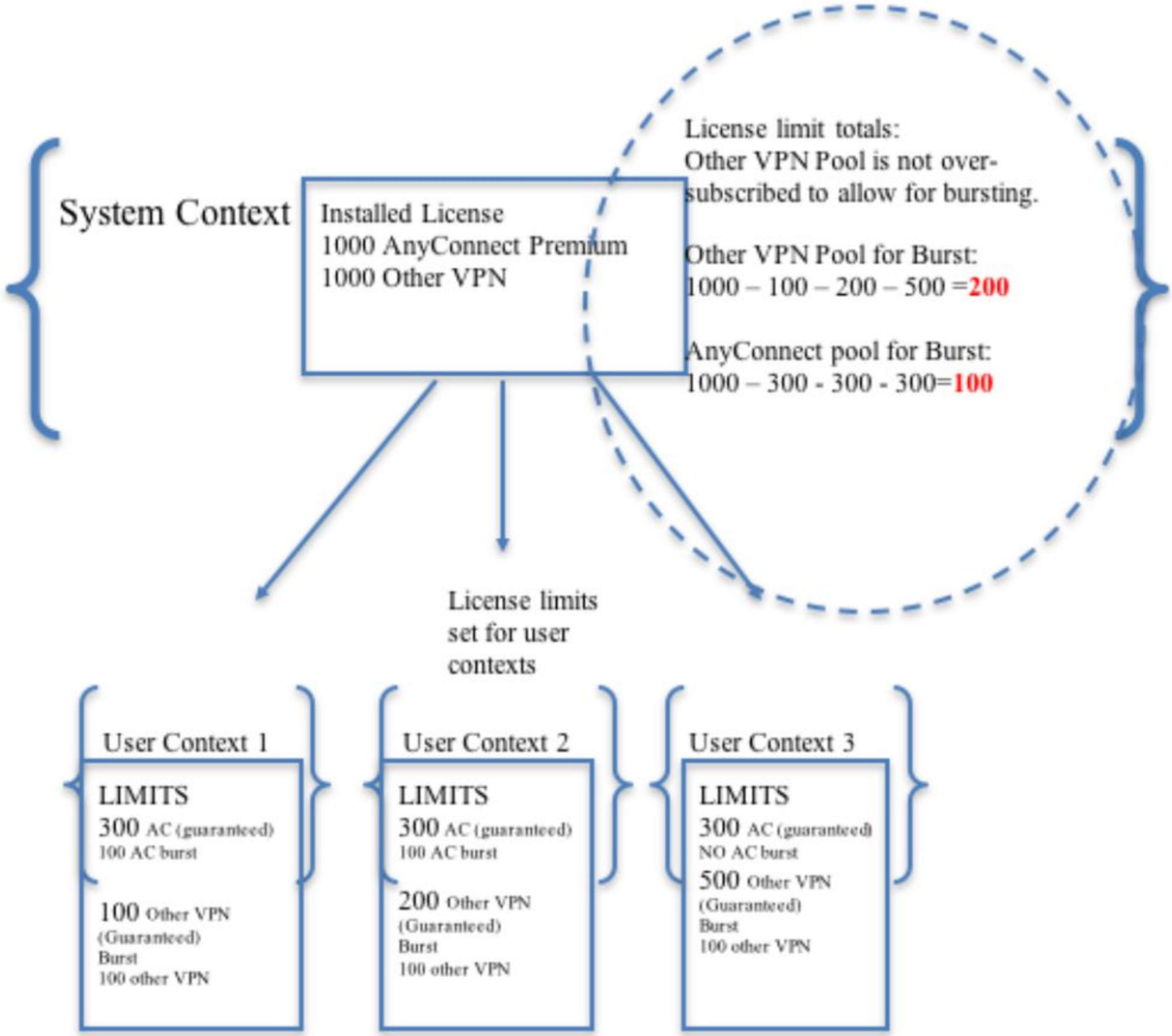
Step 2. Allocate VPN Resouce.

Configured via existing class configuration. Licenses are allowed by the number of licenses or % of total per context

New resource types introduced for MC RAVPN:

- VPN AnyConnect: Guaranteed to a context and can’t be oversubscribed
- VPN Burst AnyConnect: Allow context extra licenses beyond the guaranteed limit. Burst pool consists of any licenses not guaranteed to a context and are allowed to a bursting context on a first-come-first-serve basis

VPN License Provisioning model:



Note: ASA5585 offers 10,000 maximum Cisco AnyConnect user sessions and in this example, 4000 Cisco AnyConnect user session is allocated per context.

```
class resource02
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000

class resource01
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000
```

Step 3. Configure contexts and assign resources.

Note: In this example GigabitEthernet0/0 is shared among all the context.

```
admin-context admin
```

```
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Step 4. Verify that Apex License is installed on the ASA, refer below link for more details.

Activating or Deactivating Activation Keys

Step 5. Configure an Anyconnect image package. Depending on which ASA version is being used, there are two ways load Anyconnect image and configure for RA VPN. If the version is 9.6.2 and above, Flash virtualization can be used. For older versions than 9.6.2 refer Appendix A

> **Note:** On 9.6.2 and above we have support for Flash Virtualization which means we can have Anyconnect image per context.

Flash Virtualization

Remote-access VPN requires flash storage for various configuration and images like AnyConnect packages, hostscan packages, DAP configuration, plugins, customization and localization, etc. In multi-context mode before 9.6.2, user contexts cannot access any part of the flash and the flash is managed and accessible to the system administrator via the system context only.

In order to resolve this limitation, while still maintaining security and privacy of files on the flash as well as being able to share the flash fairly among contexts, a virtual file system is created for the flash in multi-context mode. The purpose of this feature is to allow AnyConnect images to be configured on a per-context basis rather than have them configured globally. This allows different users to have different AnyConnect images installed. In addition, by allowing AnyConnect images to be shared, the amount of memory consumed by these images can be reduced. The shared storage is used to store files and packages that are common to all contexts.

> **Note:** The system context administrator will continue to have full read-write access to the entire flash and the private and shared storage file systems.The system administrator will need to create a directory structure and organize all private files and shared files into different directories so that these directories can be configured for contexts to access as shared storage and private storage respectively.

Every context will have read/write/delete permission to its own private storage and will have read-only access to its shared storage. Only the system context will have write access to the shared storage.

In the below configs, Custom Context 1 will be configured to illustrate private storage, and Custom Context 2 will be configured to illustrate shared storage.

Private storage

You can specify one private storage space per context. You can read/write/delete from this directory within the context (as well as from the system execution space). Under the specified path, the ASA creates a sub-directory named after the context.

For example, for context1 if you specify disk0:/private-storage for the path, then the ASA creates a sub-directory for this context at disk0:/private-storage/context1/.

Shared storage

One read-only shared storage space can be specified per context. To reduce duplication of common large files that can be shared among all contexts (such as AnyConnect packages), shared storage space can be used.

Configurations to use the private storage space

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

Configurations to use the shared storage space

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

Verify the image under the respective contexts

```
!! Custom Context 1 configured for private storage.

ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

!! Custom Context 2 configured for shared storage.
```

```
ciscoasa(config)#changeto context context2
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

Step 6. Below is the summary of the configurations in the system Context that includes the flash virtualization configs described above:

System Context

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
 storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

Step 7: Configure the two custom contexts as shown below

Custom Context 1

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
```

```
group-alias MC_RAVPN_1 enable
```

Custom Context 2

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0
username cisco password cisco

!! Configure the required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com
!
!
tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

Verify

Use this section in order to confirm that your configuration works properly.

Verify If Apex License is Installed

ASA does not specifically recognise an AnyConnect Apex license but it enforces license characteristics of an Apex license which include:

- AnyConnect Premium licensed to the platform limit
- AnyConnect for Mobile
- AnyConnect for Cisco VPN Phone
- Advanced Endpoint Assessment

A syslog will be generated when a connection is blocked because an AnyConnect Apex license is not installed.

Verify If AnyConnect Package is available in custom contexts (9.6.2 and above)

```
! AnyConnect package is available in context1

 ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

In case, the image is not present under the custom context please refer Anyconnect image configuration (9.6.2 and above).

Verify If Users can connect via AnyConnect on custom contexts

> **Tip:** For better display watch below videos in full screen.

```
!! One Active Connection on Context1

ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 5
Assigned IP : 192.168.1.1 Public IP : 10.142.168.102
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Mobile
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 3186 Bytes Rx : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time : 15:33:25 UTC Thu Dec 3 2015
Duration : 0h:00m:05s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : cisco Index : 1
Assigned IP : 192.168.51.1 Public IP : 10.142.168.94
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 10550 Bytes Rx : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time : 15:34:16 UTC Thu Dec 3 2015
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
Status : Capacity : Installed : Limit
-----------------------------------------
AnyConnect Premium : ENABLED : 10000 : 10000 : NONE
Other VPN (Available by Default) : ENABLED : 10000 : 10000 : NONE
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment : ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone : ENABLED
VPN-3DES-AES : ENABLED
VPN-DES : ENABLED
----------------------------------------------------------------------------

----------------------------------------------------------------------------
VPN Licenses Usage Summary
----------------------------------------------------------------------------
Local : Shared : All : Peak : Eff. :
In Use : In Use : In Use : In Use : Limit : Usage
-----------------------------------------------------
AnyConnect Premium : 2 : 0 : 2 : 2 : 10000 : 0%
AnyConnect Client : : 2 : 2 : 0%
AnyConnect Mobile : : 2 : 2 : 0%
Other VPN : : 0 : 0 : 10000 : 0%
Site-to-Site VPN : : 0 : 0 : 0%
----------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource Current Peak Limit Denied Context
AnyConnect 1 1 4000 0 context1
AnyConnect 1 1 4000 0 context2
```

Troubleshoot

This section provides the information you can use in order to troubleshoot your configuration.

Troubleshooting AnyConnect

> **Tip:** In case ASA does not have Apex License installed, AnyConnect session would be terminated with below syslog:
>
> %ASA-6-725002: Device completed SSL handshake with client

```
OUTSIDE:10.142.168.86/51577 to 10.106.44.38/443 for TLSv1 session
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-6-113009: AAA retrieved default group policy (GroupPolicy_MC_RAVPN_1) for user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-3-716057: Group User IP <10.142.168.86> Session terminated, no AnyConnect Apex license available
%ASA-4-113038: Group User IP <10.142.168.86> Unable to create AnyConnect parent session.
```

Appendix A - Anyconnect image configuration for versions before 9.6.2

The AnyConnect image is configured globally in the admin context for ASA versions before 9.6.2 (note that the feature is available from 9.5.2) because the flash storage is not virtualized and it is only accessible from the system context.

Step 5.1. Copy AnyConnect package file to the flash in the system context.

System Context:

```
ciscoasa(config)# show flash:

195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

Step 5.2. Configure the Anyconnect image in the Admin context.

Admin Context::

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

Note: Anyconnect image could be configured in the admin context only. All contexts automatically refer to this global Anyconnect image configuration.

Custom Context 1:

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.38 255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration
```

```
ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
banner value "Welcome to Context1 SSLVPN"
wins-server none
dns-server value 192.168.20.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
group-alias MC_RAVPN_1 enable
group-url https://10.106.44.38/context1 enable
```

Custom Context 2:

```
!! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
nameif OUTSIDE
security-level 0
ip address 10.106.44.36 255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
enable OUTSIDE
anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
banner value "Welcome to Context2 SSLVPN"
wins-server none
dns-server value 192.168.60.10
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
address-pool mypool
default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
group-alias MC_RAVPN_2 enable
```

```
group-url https://10.106.44.36/context2 enable
```

Verify If AnyConnect Package is installed in Admin Context and is available in custom contexts (before 9.6.2)

```
!! AnyConnect package is installed in Admin Context

ciscoasa/pri/admin/act# show run webvpn
webvpn
anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1

ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable OUTSIDE
anyconnect enable
tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
CISCO STC win2k+
3,1,10010
Hostscan Version 3.1.10010
Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

References

Release Notes: 9.5(2)

Release Notes: 9.6(2)

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **AnyConnect VPN Client Troubleshooting Guide - Common Problems**
- **Managing, Monitoring, and Troubleshooting AnyConnect Sessions**
- **Technical Support & Documentation - Cisco Systems**
- **https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf**