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

Inleiding

Dit document beschrijft hoe u de firewall van Cisco Adaptieve security applicatie (ASA) in Multicontext (MC) kunt configureren met behulp van de CLI-modus (Remote Access Network). Het toont Cisco ASA in meerdere context-mode ondersteunde/niet-ondersteunde functies en licentievereisten met betrekking tot RA VPN.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ASA AnyConnect SSL-configuratie
- ASA configuratie van meerdere Context

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AnyConnect Secure Mobility Client versie 4.4.0243
- Twee ASA 5525 met ASA-software versie 9.6(2)

  Opmerking: Download het AnyConnect VPN-clientpakket van de Cisco Software Download (alleen geregistreerde klanten).

  Opmerking: De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Multi-context is een vorm van virtualisatie waarmee meerdere onafhankelijke exemplaren van een toepassing tegelijkertijd op dezelfde hardware kunnen worden uitgevoerd, waarbij elke kopie (of virtueel apparaat) als een afzonderlijk fysiek apparaat voor de gebruiker verschijnt. Hierdoor kan één ASA als meerdere ASA's verschijnen aan meerdere onafhankelijke gebruikers. De ASA-familie heeft virtuele firewalls ondersteund sinds de eerste vrijgave ervan. er was echter geen virtualisatieondersteuning voor externe toegang in de ASA. VPN LAN2LAN (L2L)-ondersteuning voor multicontext is toegevoegd voor de 9.0-release.

Opmerking: Van 9.5.2 op multicontext gebaseerde virtualisatieondersteuning voor VPN Remote Access (RA)-verbindingen naar de ASA.

Vanaf 9.6.2 hebben we ondersteuning voor Flash virtualisatie wat betekent dat we AnyConnect-beeld per context kunnen hebben.

Historie voor functies voor multicontext

Nieuwe functies toegevoegd in ASA 9.6(2)

Functie	Beschrijving
Voorgevulde/achternaam-van-bron optie voor meerdere contextmodus	AnyConnect SSL-ondersteuning wordt uitgebreid, zodat ook CLI's die voorheen alleen in één modus beschikbaar waren, kunnen worden ingeschakeld in meerdere contextmodus.
Flash-virtualisatie voor externe toegang VPN	VPN-toegang op afstand in meerdere context ondersteunt flash-virtualisatie nu. Elke context kan een privéopslagruimte en een gedeelde opslagplaats hebben op basis van de totale beschikbare flitser.
AnyConnect-clientprofielen ondersteund in multicontext-apparaten	AnyConnect-clientprofielen worden ondersteund in multi-context-apparaten. Als u een nieuw profiel wilt toevoegen met ASDM, moet u minimaal de AnyConnect Secure Mobility Client release 4.2.00748 of 4.3.030/13 hebben.
Stateful failover voor AnyConnect-verbindingen in multi-contextmodus	Stateful failover wordt nu ondersteund voor AnyConnect-verbindingen in meerdere contextmodus.
Remote Access VPN Dynamic Access Policy (DAP) wordt ondersteund in multi-context-modus	U kunt nu DAP per context in meerdere contextmodus configureren.
Remote Access VPN-CoA (verandering van autorisatie) wordt ondersteund in meerdere context-modus	U kunt CoA per context nu configureren in meerdere context-modus.
Remote Access VPN-localisatie wordt ondersteund in multi-context-modus	Localisatie wordt wereldwijd ondersteund. Er is slechts één set localisatiebestanden die over verschillende contexten worden gedeeld.
Opslagopslag per context wordt ondersteund.	Het doel van deze functie is om de gebruiker in staat te stellen om een opname rechtstreeks van een context naar de externe opslag te kopiëren of naar de context privé-opslag op flitser. Deze optie stelt het ook mogelijk om de ruwe opname naar de externe gereedschappen voor pakketvastlegging zoals draadscherf van binnen een context te kopiëren.

Functies in ASA 9.5(2)

Functie	Beschrijving
AnyConnect 4.x en hoger (alleen SSL VPN) geen IKEv2-	Ondersteuning voor multi-context-gebaseerde virtualisatie voor VPN Remote Access (RA)-verbindingen met de ASA.

ondersteuning)	
Gecentraliseerde AnyConnect-beeldconfiguratie	• Flitsopslag wordt niet gevirtualiseerd. • AnyConnect-afbeelding wordt wereldwijd in de beheercontext geconfigureerd en de configuratie is op alle contexten van toepassing
AnyConnect-afbeeldingsupgrade	AnyConnect-clientprofielen worden ondersteund in multi-context-apparaten. Als u een nieuw profiel wilt toevoegen met ASDM, moet u minimaal de AnyConnect Secure Mobility Client release 4.2.00748 of 4.3.030/13 hebben.
Context Resource Management voor AnyConnect-verbindingen	• Configureerbaarheid om maximale licentieverbruikbaarheid per context te controleren • Configureerbaar om licentieverwerking per context toe te staan

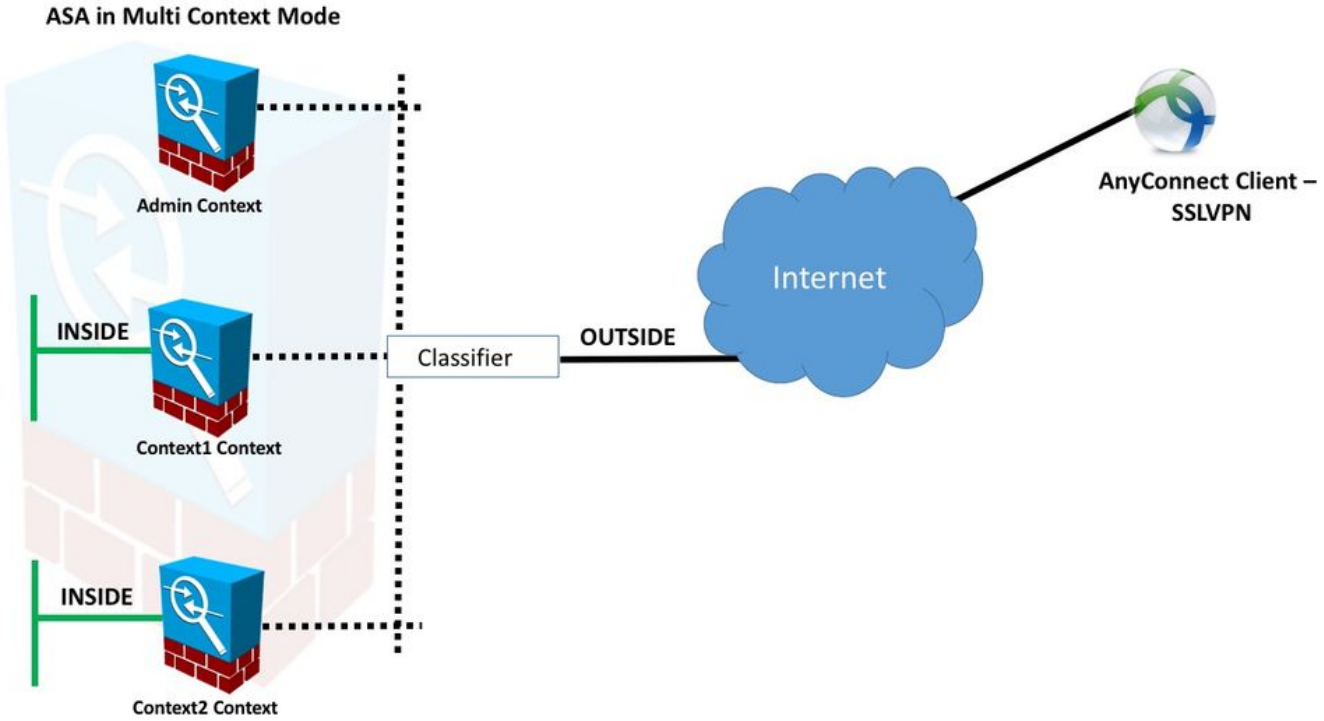
Licentie

- AnyConnect Apex-licentie vereist
- Vergunningen in wezen genegeerd/niet toegestaan
- Configureerbaarheid om maximale licentieverbruikbaarheid per context te controleren
- Configureerbaar om licentieverwerking per context toe te staan

Configureren

Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Opmerking: Meerdere contexten in dit voorbeeld delen een interface (BUITEN) en dan gebruikt de klassieker de interface unieke (auto of handleiding) MAC adressen om pakketten door te sturen. Voor meer informatie over de manier waarop security applicaties pakketten in meerdere context indelen, raadpleeg hoe de ASA Packets indeelt

De volgende configuratieprocedure is in ASA 9.6.2 versie en hoger, wat een aantal van de beschikbare nieuwe functies illustreert.De verschillen in de configuratieprocedure voor ASA-versies vóór 9.6.2 (en boven 9.5.2) zijn gedocumenteerd in Bijlage A van het document.

De benodigde configuraties in systeemcontext en aangepaste contexten voor het instellen van VPN-toegang op afstand worden hieronder beschreven:

Eerste configuraties in systeemcontext

Om te beginnen, in de configuratie van de Context van het Systeem, de toewijzing van de middelen van VPN, douanecontexten en de controle van de Apex- vergunning. De procedure en de configuraties worden beschreven in dit gedeelte en in de volgende sectie

Stap 1. Configuratie failover

```
 !! 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
```

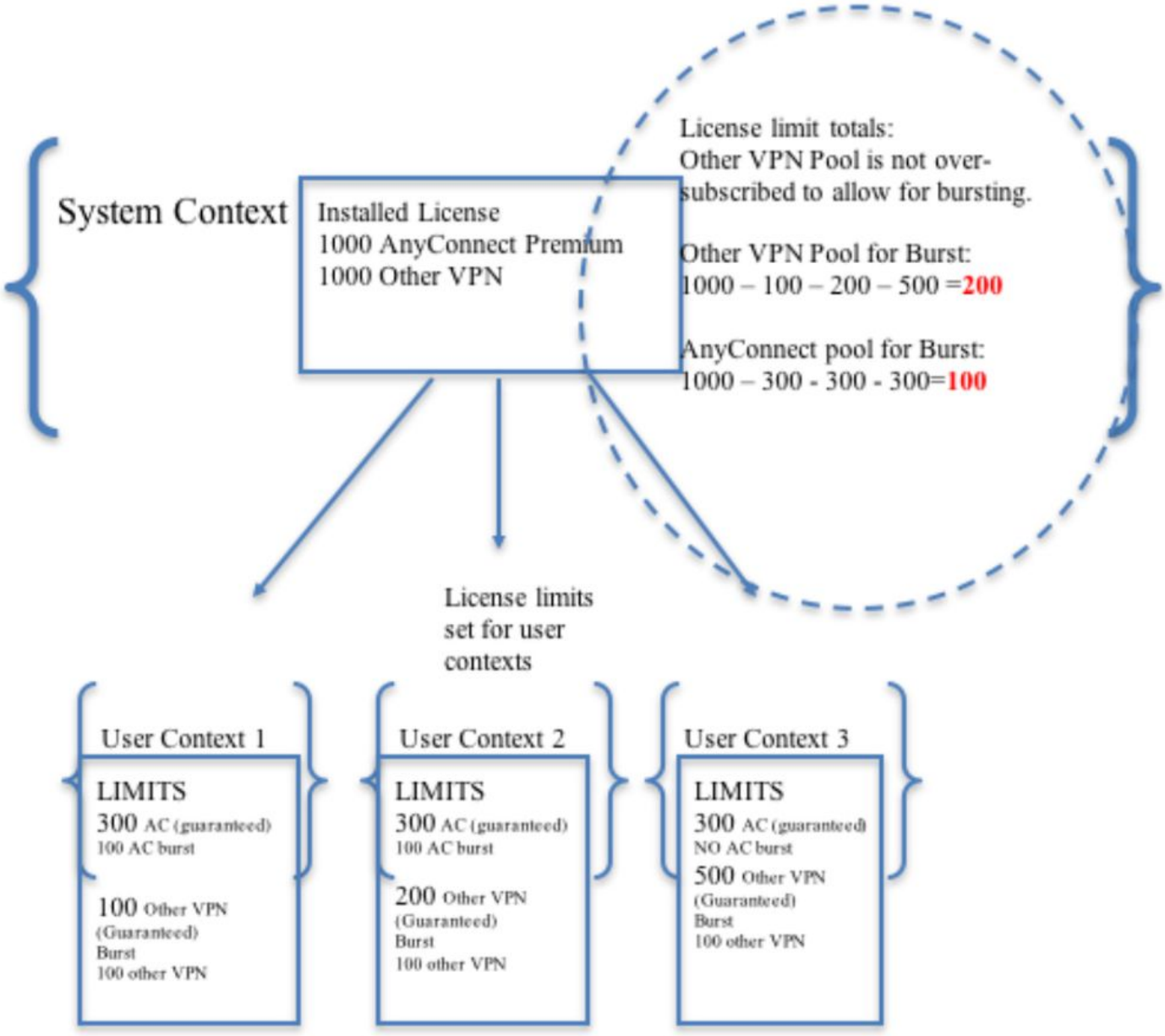
Stap 2. Wijzig VPN-middelen.

Configureerd via bestaande class-configuratie. De certificaten zijn toegestaan op basis van het aantal vergunningen of % van het totale aantal vergunningen per context

Nieuwe resource typen voor MC RAVPN geïntroduceerd:

- VPN AnyConnect: Gegarandeerd aan een context en kan niet worden overschreden
- VPN Burst AnyConnect Toestaan van contextextra licenties boven de gegarandeerde limiet. Burst pool bestaat uit alle licenties die niet gegarandeerd zijn aan een context en die toegestaan zijn om een barstende context te bereiken op basis van de eerste-aanloopfase

VPN License Provisioning model:



Opmerking: ASA 5585 biedt 10.000 maximale Cisco AnyConnect-gebruikerssessies en in dit voorbeeld worden 4000 Cisco AnyConnect-gebruikerssessies per context toegewezen.

```
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
```

Stap 3. Het configureren van contexten en het toewijzen van resources.

Opmerking: In dit voorbeeld wordt Gigabit Ethernet0/0 onder alle context gedeeld.

```
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
```

Stap 4. Controleer dat de Apex-licentie op de ASA is geïnstalleerd en raadpleeg de onderstaande link voor meer informatie.

Activeringstoetsen in- of uitschakelen

Stap 5. Configureer een beeldpakket met AnyConnect. Afhankelijk van de vraag of de ASA versie wordt gebruikt, zijn er twee manieren om AnyConnect-afbeelding te laden en voor RA VPN te configureren. Als de versie 9.6.2 en hoger is, kan Flitser virtualisatie worden gebruikt. Voor oudere versies dan 9.6.2 zie Bijlage A

> Opmerking: Op 9.6.2 en hoger hebben we ondersteuning voor Flash Virtualization, wat betekent dat we AnyConnect Image per context kunnen hebben.

Flitsvirtualisatie

VPN-toegang op afstand vereist flash-opslag voor verschillende configuratie en afbeeldingen, zoals AnyConnect-pakketten, hostscan-pakketten, DAP-configuratie, plug-ins, aanpassing en localisatie, enzovoort. In multi-context-modus vóór 9.6.2 hebben gebruikers geen toegang tot een deel van de flitser en is de flitser alleen via de systeemcontext beheerd en toegankelijk voor de systeembeheerder.

Om deze beperking op te lossen, terwijl de veiligheid en privacy van bestanden op de flitser nog steeds behouden en de flitser eerlijk tussen contexten kunnen delen, wordt er een virtueel bestandssysteem gemaakt voor de flitser in multi-context-modus. Het doel van deze functie is om AnyConnect-afbeeldingen op een per-context-basis te laten configureren in plaats van ze mondiaal te laten configureren. Hierdoor kunnen verschillende gebruikers verschillende AnyConnect-afbeeldingen laten installeren. Bovendien kan de hoeveelheid geheugen die door deze afbeeldingen wordt geconsumeerd, worden verminderd door AnyConnect-afbeeldingen te delen. De gedeelde opslag wordt gebruikt om bestanden en pakketten op te slaan die voor alle contexten gemeenschappelijk zijn.

> Opmerking: De systeembeheerder zal volledige lees-schrijftoegang blijven hebben tot de gehele flitser en het privé en gedeelde opslagbestandssysteem.De systeembeheerder zal een directory-structuur moeten maken en alle privé bestanden en gedeelde bestanden in verschillende directories moeten organiseren, zodat deze directories kunnen worden

geconfigureerd voor toegang tot respectievelijk gedeelde opslag en privé-opslag.

Elke context heeft een lees-schrijf/verwijder toestemming voor zijn eigen privéopslag en heeft alleen-lezen toegang tot de gedeelde opslag. Alleen de systeemcontext heeft toegang tot de gedeelde opslag.

In de onderstaande configuratie wordt Aangepaste Context 1 geconfigureerd om particuliere opslag te illustreren, en Aangepaste Context 2 wordt geconfigureerd om gedeelde opslag te illustreren.

Particuliere opslag

U kunt per context één particuliere opslagruimte instellen. U kunt deze map binnen de context lezen/schrijven/verwijderen (en ook vanuit de ruimte voor systeemuitvoering). Onder het gespecificeerde pad maakt de ASA een subdirectory genaamd naar de context.

Bijvoorbeeld, voor context1 als u disk0:/private opslag voor het pad specificeert, dan creëert de ASA een subdirectory voor deze context op disk0:/private opslag/context1/.

Gedeelde opslag

Eén alleen-lezen gedeelde opslagruimte kan per context worden gespecificeerd. Om doublures van gemeenschappelijke grote bestanden te voorkomen die onder alle contexten kunnen worden gedeeld (zoals AnyConnect-pakketten), kan gedeelde opslagruimte worden gebruikt.

Configuraties om de particuliere opslagruimte te gebruiken

```
!! 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
```

Configuraties om de gedeelde opslagruimte te gebruiken

```
!! 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
```

Controleer de afbeelding onder de respectieve contexten

```
!! 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
```

Stap 6. Hieronder volgt de samenvatting van de configuraties in de systeemcontext die de hierboven beschreven flitsvirtualisatie-configuraties bevat:

Systeemcontext

```
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
```

Stap 7: De twee aangepaste contexten configureren zoals hieronder weergegeven

Aangepaste 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
```

Aangepaste 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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Controleer of de Apex-licentie is geïnstalleerd

ASA erkent een AnyConnect Apex-licentie niet specifiek, maar handhaaft wel de licentiekenmerken van een Apex-licentie, waaronder:

- AnyConnect Premium waarvoor een vergunning is verleend aan de platformgrens
- AnyConnect voor mobiel
- AnyConnect voor Cisco VPN-telefoon

- Geavanceerde endpointevaluatie

Er wordt een beveiliging gegenereerd wanneer een verbinding is geblokkeerd omdat er geen AnyConnect Apex-licentie is geïnstalleerd.

Controleer of AnyConnect Package beschikbaar is in een aangepaste context (9.6.2 en hoger)

```
! 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
```

Als het beeld niet aanwezig is onder de aangepaste context, raadpleegt u Any-Connect beeldconfiguratie (9.6.2 en hoger).

Controleer of gebruikers zich via AnyConnect kunnen aansluiten op een aangepaste context

> **Tip:** Bekijk onderstaande video's op het volledige scherm voor een beter beeld.

```
!! 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 : 0a6a2c24000010005660 60f8
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
```

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

AnyConnect voor probleemoplossing

> **Tip:** Indien ASA Apex License niet heeft geïnstalleerd, wordt AnyConnect-sessie met onderstaande tekst beëindigd:
>
> %ASA-6-72502: Apparaat voltooide SSL-handdruk met client BUITEN:10.142.168.86/51577 tot 10.106.44.38/443 voor TLSv1-sessie
> %ASA-6-113012: AAA-gebruikersverificatie geslaagd: lokale databank : gebruiker = cisco
> %ASA-6-11309: AAA herwon standaard groepsbeleid (GroupPolicy_MC_RAVPN_1) voor gebruiker = cisco
> %ASA-6-11308: AAA-transactiestatus ACCEPTEERT : gebruiker = cisco
> %ASA-3-716057: IP-sessie van groepsgebruiker <10.142.168.86> beëindigd, geen AnyConnect Apex-licentie beschikbaar
> %ASA-4-113038: IP-groepsgebruiker <10.142.168.86> Kan geen AnyConnect oudersessie maken.

Bijlage A - AnyConnect-beeldconfiguratie voor versies vóór 9.6.2

De AnyConnect-afbeelding wordt voor ASA-versies wereldwijd voorafgaand aan 9.6.2 geconfigureerd in de beheercontext (opmerking dat de functie beschikbaar is vanaf 9.5.2) omdat de flash-opslag niet virtueel is en alleen toegankelijk is vanuit de systeemcontext.

Stap 5.1. Kopieer AnyConnect-pakketbestand naar de flitser in de systeemcontext.

Systeemcontext:

```
ciscoasa(config)# show flash:

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

Stap 5.2. De AnyConnect-afbeelding configureren in de Admin-context.

Context beheren:

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

Opmerking: AnyConnect-afbeelding kan alleen in de beheercontext worden ingesteld. Alle contexten verwijzen automatisch naar deze mondiale AnyConnect-beeldconfiguratie.

Aangepaste 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
```

Aangepaste 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
```

Controleer of AnyConnect Package in Admin Context is geïnstalleerd en in een aangepaste context beschikbaar is (vóór 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
```

Referenties

Releaseopmerkingen: 9.5(2)

Releaseopmerkingen: 9.6(2)

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties

- AnyConnect VPN-clientprobleemoplossing - gemeenschappelijke problemen
- AnyConnect-sessies beheren, controleren en probleemoplossing
- Technische ondersteuning en documentatie – Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf