Statische IP-adrestoewijzing voor beveiligde client-VPN-gebruikers configureren

Inhoud

leiding	
<u>borwaarden</u>	
Vereisten	
Gebruikte componenten	
chtergrondinformatie	
onfigureren	
erifiëren	
oblemen oplossen	

Inleiding

Dit document beschrijft hoe statische IP-adressen aan externe VPN-gebruikers kunnen worden toegewezen door gebruik te maken van een LDAP-kenmerkkaart.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Active Directory (AD)
- Lichtgewicht Directory Access Protocol (LDAP)
- Cisco Secure Firewall-bescherming tegen bedreigingen
- Cisco Secure Firewall Management Center

Gebruikte componenten

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

- Windows Server 2022
- FTD versie 7.4.2
- FMC versie 7.4.2

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Opmerking: De optie om een Realm voor IP-adrestoewijzing te gebruiken en LDAP attribuut maps te configureren wordt ondersteund in FirePOWER versie 6.7 of hoger. Zorg ervoor dat de FirePOWER-versie 6.7 of hoger is voordat u verdergaat.

Configureren

Stap 1. Navigeer naar Apparaten > Externe toegang en selecteer het gewenste VPN-beleid voor externe toegang. Selecteer het gewenste verbindingsprofiel. Selecteer onder het tabblad AAA een Realm voor verificatieserver en autorisatieserver.

Edit Connection Profile		0
Connection Profile:* Group Policy:*	RAVPN_PROFILE +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method: Authentication Server:	WINDOWS_2022_AD (AD) +	
Use secondary authenticat	Fallback to LOCAL Authentication	
Authorization		
Authorization Server:	Use same authentication server	
Accounting		
Accounting Server:	· ·	- 1
 Advanced Settings 		
	Cancel Sav	/e

Stap 2. Navigeer naar Apparaten > Externe toegang en selecteer het gewenste Remote Access VPN-beleid. Navigeer naar Advanced > Address Assignment Policy en controleer of de optie Use autorisatieserver (Alleen voor RADIUS of Real) is ingeschakeld.



Stap 3. Navigeer naar Geavanceerd > Toewijzing van LDAP-kenmerken en voeg een Naamkaart toe waarvan de naam van LDAP-kenmerken is ingesteld op msRADIUSFramedIPAaddress en de naam van Cisco-kenmerken is ingesteld op IETF-Radius-Framed-IP-Address.

Firewall Managemen Devices / VPN / Edit Advance	nt Center Overview	Analysis	Policies Devices	Objects	Integration		Deploy 🔍 💞 🌣 🔕	admin ~ de-de- SECURE
RAVPN_POLICY								Save Cancel
Enter Description								
								Policy Assignments (1)
							Local Realm: None	Dynamic Access Policy: None
Connection Profile Access Inte	erfaces Advanced							
Secure Client Images	LDAP Attribute Mapping							
Secure Client Customization	LDAP attribute mapping can be c	onfigured to enabl	le LDAP server to perform	authorization.				
GUI Text and Messages								+
lcons and Images	Realm		м	ар				
Scripts	WARDOWE 1993 AD		N	ame:				/ 3
Binaries	11100110_2022_00			msRADIUSFran	medIPAddress -> IETF-Radius-Framed-IP-Address			
Custom Installer Transforms			Configure LDA	P Attribute Ma	p	0		
Localized Installer Transforms								
Address Assignment Policy			Realm:					
Certificate Maps			WINDOWS_2023	(_AD (AD) *				
Group Policies			1010					
LDAP Attribute Mapping			LDAP attribute Maj	25:		÷		
Load Balancing			Name Map:			1.1		
✓ IPsec			LDAP Attribute 1	Jame	Cisco Attribute Name			
Crypto Maps			mskADiUSFra	mediPAddress	▼ IETF-Radius-Framed-IP'-Address▼			
IKE Policy			Value Maps:					
IPsec/IKEv2 Parameters			LDAP Attribute \	/alue	Cisco Attribute Value			
					Add Value Map			
						_		
					Cancel	ОК		

Stap 4. Open Server Manager op uw Windows AD-server en navigeer naar Tools > Active Directory-gebruikers en computers. Klik met de rechtermuisknop op een gebruiker, selecteer Eigenschappen > Inbellen en controleer het vakje Statische IP-adressen toewijzen.

Jo	hn	Doe	Pro	perties

Remote co	ontrol	Remote D	esktop Se	rvices Profile	COM+
General	Address	Account	Profile	Telephones	Organization
Member (Df	Dial-in	Envi	ronment	Sessions
Network A C Allow a C Deny a C Control	ccess Pem ccess ccess access thr	nission ough NPS Ne	twork Polic	⊃y	
Callback O Callback O No Cal Set by Always	Caller-ID: Options Iback Caller (Rou Callback t	iting and Rem	ote Acces	s Service only)	
Define IP Dial-in cor	Static IP A addresses nnection.	ddresses — to enable for t	his	Static IP Addre	esses
Define rou connectio	itatic Route Ites to enal n.	es ble for this Dia	l-in	Static R	outes
	OK	(C	ancel	Apply	Help

Stap 5. Selecteer Statische IP-adressen en wijs een statisch IP-adres aan de gebruiker toe.

Static IP Addresses	×
Assign a static IPv4 address:	172 . 16 . 20 . 73
Assign a static IPv6 address:	
Prefix:	
Interface ID:	
OK	Cancel

Stap 6. Maak verbinding met de VPN-gateway en log-in met de Cisco Secure-client. De gebruiker krijgt het statische IP-adres toegewezen dat u hebt geconfigureerd.

S Cisco Secure Client		-		×
cisco Secure (Client			0
General	Virtual Private Network (VPN)			
Status Overview	Preferences Statistics Route Details Firewall Message History			
AnyConnect VPN >	Connection Information		- •	^
Zero Trust Access	State: Connected Tunnel Mode (IPv4): Tunnel All Traffic Tunnel Mode (IPv6): Drop All Traffic			
Network	Dynamic Tunnel Exclusion: None Dynamic Tunnel Inclusion: None			
ISE Posture	Duration: 00:00:26 Session Disconnect: None			
Umbrella	Management Connection State: Disconnected (user tunnel active) Address Information		_ ^	
Collect diagnostic information for all	Client (IPv4): 172.16.20.73 Client (IPv6): Not Available Server: 10.0.0.1 Bytes		_ ^	~
Diagnostics	Reset	Exp	port Stats	

Verifiëren

Schakel debug ldap 255 in en controleer of het kenmerk msRADIUSFramedIPAddress LDAP wordt opgehaald:

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

```
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dSCorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

Problemen oplossen

Opdrachten voor debugging:

debug webvpn 255

debug ladder

Opdracht om het statische IP-adres te valideren dat is toegewezen aan de gewenste RA VPNgebruiker:

toon vpn-sessiondb om het even welke verbindingsfilternaam <gebruikersnaam>

<#root>

firepower#

show vpn-sessiondb anyconnect filter name jdoe

Session Type: AnyConnect

```
Username : jdoe Index : 7

Assigned IP : 172.16.20.73 Public IP : 10.0.0.10

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384

Bytes Tx : 14664 Bytes Rx : 26949

Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE

Login Time : 11:45:48 UTC Sun Sep 29 2024

Duration : Oh:38m:59s

Inactivity : Oh:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : cb0071820000700066f93dec

Security Grp : none Tunnel Zone : 0
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.