Invoeren van harde maatregelen voor beveiligde client-AnyConnect VPN

Inhoud

| Inleiding |
|---|
| Voorwaarden |
| Vereisten |
| Gebruikte componenten |
| Achtergrondinformatie |
| Concepten |
| Beveiligde praktijken voor clientharding op Cisco Secure Firewall: |
| Identificeer aanvallen met vastlegging- en syslog-id's |
| Aanvalsverificatie |
| FMC-configuratievoorbeelden |
| AAA-verificatie uitschakelen in de standaard-WEBVPNG-groep en DefaultRAGroup- verbindingsprofielen |
| Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel) |
| Groepsaliassen uitschakelen en Groep-URL's inschakelen |
| Toewijzing van certificaten |
| IPsec-IKEv2 |
| ASA-configuratievoorbeelden |
| AAA-verificatie uitschakelen in de standaard-WEBVPNG-groep en DefaultRAGroup- verbindingsprofielen |
| Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel) |
| Groepsaliassen uitschakelen en Groep-URL's inschakelen |
| Toewijzing van certificaten |
| IPsec-IKEv2 |
| Conclusie |
| Gerelateerde informatie |
| |

Inleiding

Dit document beschrijft hoe u de beveiliging van uw implementatie van Remote Access VPN kunt verbeteren.

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Cisco Secure-client voor AnyConnect VPN.
- ASA/FTD-configuratie voor externe toegang.

Gebruikte componenten

De best practices guide is gebaseerd op deze hardware- en softwareversies:

- Cisco ASA 9.x
- Firepower Threat Defense 7.x/FMC 7.x

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.



Waarschuwing: dit document bevat geen stappen voor Firepower Device Manager (FDM). De FDM ondersteunt alleen het wijzigen van de verificatiemethode op de DefaultWEBVPNGgroep. Gebruik ACL's (control-plane) of een aangepaste poort in de sectie 'Global Settings' van Remote Access VPN in de FDM UI. Neem contact op met het Cisco Technical Assistance Center (TAC) voor verdere assistentie, indien nodig.

Achtergrondinformatie

Het doel van dit document is om er zeker van te zijn dat de configuratie van Cisco Secure Client AnyConnect VPN voldoet aan de best practices op het gebied van beveiliging in een moderne wereld waarin cyberbeveiligingsaanvallen gebruikelijk zijn.

Brute force aanvallen impliceren gewoonlijk herhaalde pogingen om toegang tot een middel te krijgen door gebruikersbenaming en wachtwoordcombinaties te gebruiken. De aanvallers proberen hun internetbrowser, de Secure Client-gebruikersinterface of andere tools te gebruiken om meerdere gebruikersnamen en wachtwoorden in te voeren in de hoop dat ze een legitieme combinatie in een AAA-database evenaren. Bij het gebruik van AAA voor verificatie verwachten we dat de eindgebruiker zijn gebruikersnaam en wachtwoord invoert, omdat dit nodig is om de verbinding tot stand te brengen. Tegelijkertijd controleren we niet wie de gebruiker is totdat ze hun referenties invoeren. Dit stelt aanvallers van nature in staat om voordeel te halen uit deze scenario's:

- 1. Volledig gekwalificeerde domeinnamen voor de Cisco Secure Firewall (met name bij gebruik van een groepsalias in het verbindingsprofiel):
 - Als de aanvaller de FQDN van uw VPN-firewall ontdekt, hebben ze de optie om de tunnelgroep te selecteren met behulp van de groep-alias waarin ze de bruteforce aanval willen starten.
- 2. Standaardverbindingsprofiel geconfigureerd met AAA of Local Database:
 - Als de aanvaller de FQDN van de VPN-firewall vindt, kan hij proberen brute-force aanvallen op de AAA-server of lokale database. Dit gebeurt omdat de verbinding met de FQDN op het Default Connection Profile landt, zelfs als er geen groepaliassen zijn gespecificeerd.
- 3. Resourcetest op de firewall of op AAA-servers:
 - Aanvallen kunnen AAA-servers of firewallbronnen overweldigen door grote hoeveelheden verificatieverzoeken te verzenden en een Denial of Service (DoS)voorwaarde te maken.

Concepten

Groepsaliassen:

• Een alternatieve naam waarmee de firewall kan verwijzen naar een verbindingsprofiel. Na het initiëren van een verbinding met de firewall, verschijnen deze namen in een vervolgkeuzemenu in de Secure Client UI voor gebruikers om te selecteren. Door het verwijderen van groepsaliassen wordt de vervolgkeuzefunctie in de Secure Client UI

verwijderd.

Groep-URL's:

 Een URL die kan worden gekoppeld aan een verbindingsprofiel, zodat inkomende verbindingen direct worden toegewezen aan een gewenst verbindingsprofiel. Er is geen vervolgkeuzefunctie, aangezien gebruikers de volledige URL in de Secure Client UI kunnen invoeren, of de URL kan worden geïntegreerd met een 'Display Name' in het XML-profiel om de URL van de gebruiker te verbergen.

Het verschil is dat wanneer groepsaliassen worden geïmplementeerd, een gebruiker een verbinding to vpn_gateway.example.com start en met aliassen wordt voorgesteld om die aliassen naar een verbindingsprofiel te selecteren. Met groep-URL's start een gebruiker een verbinding naar vpn_gateway.example.com/example_group en die stuurt ze rechtstreeks naar het verbindingsprofiel zonder dat er een vervolgkeuzemenu nodig of optioneel is.

Beveiligde praktijken voor clientharding op Cisco Secure Firewall:

Deze methodes zijn gebaseerd op het in kaart brengen van legitieme gebruikers aan juiste tunnelgroepen/verbindingsprofielen terwijl potentieel kwaadaardige gebruikers worden verzonden naar een val tunnelgroep die wij vormen om gebruikersbenaming en wachtwoordcombinaties niet toe te staan. Hoewel niet alle combinaties moeten worden geïmplementeerd, zijn het uitschakelen van groepsaliassen en het wijzigen van de verificatiemethode van de DefaultWEBVPNGroup en DefaultRAGroup vereist om de aanbevelingen effectief te laten werken.

- Schakel groepsaliassen uit en gebruik alleen groep-url in de configuratie van het verbindingsprofiel. Hierdoor kunt u een specifieke FQDN hebben die niet gemakkelijk te ontdekken en te selecteren is voor een aanvaller, aangezien alleen de clients met de juiste FQDN in staat zijn om de verbinding te starten. Bijvoorbeeld: vpn_gateway.example.com/example_group is moeilijker te ontdekken voor een aanvaller dan vpn_gateway.example.com.
- Schakel AAA-verificatie uit in de DefaultWEBVPNGroup en DefaultRAGroup en configureer certificaatverificatie, dit voorkomt een mogelijke brute-kracht tegen de lokale database of AAA-server. De aanvaller in dit scenario zou met onmiddellijke fouten bij het proberen worden voorgesteld te verbinden. Er is geen gebruikersnaam of wachtwoordveld omdat de authenticatie is gebaseerd op certificaten, dus het stoppen van brute force pogingen. Een andere optie is om een AAA-server zonder ondersteunende configuratie te maken om een 'sinkhole' te maken voor kwaadaardige aanvragen.
- Gebruik certificaattoewijzing voor het verbindingsprofiel. Hiermee kunnen binnenkomende verbindingen worden toegewezen aan specifieke verbindingsprofielen op basis van kenmerken die van certificaten op het clientapparaat zijn ontvangen. Gebruikers die over de juiste certificaten beschikken, worden correct in kaart gebracht, terwijl aanvallers die niet voldoen aan de criteria voor het in kaart brengen naar de DefaultWEBVPNGgroep worden gestuurd.

 Het gebruik van IKEv2-IPSec in plaats van SSL veroorzaakt tunnelgroepen vertrouwen op een specifieke gebruiker-groep afbeelding in het XML-profiel. Zonder deze XML op de eindgebruikersmachine worden gebruikers automatisch naar de standaardtunnelgroep gestuurd.



Opmerking: voor meer informatie over de functionaliteit van een groepsalias, zie <u>ASA</u> <u>VPN Configuration Guide</u> en neem 'Tabel 1' in acht. Verbindingsprofielkenmerken voor SSL VPN".

Identificeer aanvallen met vastlegging- en syslog-id's

Brute-force aanvallen vertegenwoordigen de overheersende methode van het compromitteren van Verre Toegang VPNs, die zwakke wachtwoorden exploiteren om onbevoegde ingang te bereiken. Het is cruciaal om te weten hoe je signalen van een aanval herkent door gebruik te maken van het gebruik van houtkap en het evalueren van systemen. Gemeenschappelijke syslogs IDs die op een aanval kunnen wijzen indien ontmoet met abnormaal volume zijn:

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

%ASA-6-113005

<#root>

%ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = ***** : user IP =

%ASA-6-716039

<#root>

%ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.x> Authentication: rejected, Session Type: WebVPN

De gebruikersnaam is altijd verborgen totdat de opdracht Gebruikersnaam voor niet-vastlegging verbergen is geconfigureerd op ASA.



Opmerking: Dit geeft inzicht als geldige gebruikers worden gegenereerd of bekend door beledigende IP's, maar wees voorzichtig, want gebruikersnamen zijn zichtbaar in de logbestanden.

Cisco ASA-vastlegging:

Gebruikershandleiding voor Secure ASA Firewall

<u>Vastlegging</u> hoofdstuk van de configuratiehandleiding voor Cisco Secure Firewall ASA Series General Operations CLI

Cisco FTD-vastlegging:

Logboekregistratie configureren op FTD via FMC

<u>Syslog-</u>sectie <u>configureren</u> in het hoofdstuk Platform-instellingen van de configuratiehandleiding voor apparaten van Cisco Secure Firewall Management Center <u>Syslog configureren en controleren in Firepower Device Manager</u>

Sectie <u>Instellingen voor systeemvastlegging configureren</u> in het hoofdstuk Systeeminstellingen van de Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager

Aanvalsverificatie

Om te verifiëren, logt u in op de ASA of FTD Command Line Interface (CLI), voert u de opdracht show aaa-server uit en onderzoekt u of er een ongebruikelijk aantal pogingen en afgewezen verificatieaanvragen is voor een van de geconfigureerde AAA-servers:

<#root>

ciscoasa#

show aaa-server

Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time Oms
Number of authentication requests 8473575 - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - >>>> Unusual increments

<#root>

ciscoasa#

show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server Server Protocol: ldap Server Hostname: ldap-server.example.com Server Address: 10.10.10.10 Server port: 636 Server status: ACTIVE, Last transaction at unknown Number of pending requests 0 Average round trip time Oms Number of authentication requests 2228536 - - - - - >>> Unusual increments Number of authorization requests 0 Number of accounting requests 0 Number of retransmissions 0 Number of accepts 1312 Number of rejects 2225363 - - - - - >>>> Unusual increments Number of challenges 0 Number of malformed responses 0

FMC-configuratievoorbeelden

AAA-verificatie uitschakelen in de standaard-WEBVPNG-groep en DefaultRAGroupverbindingsprofielen

Navigeer naar Apparaten > Externe toegang.

| F o | Firewall Manag Werview / Dashboard | ement Center Is / Dashboard | Overview | Analysis | Policies | Devices | Objects | Integration | |
|--------------------------------|---|--|----------|-------------|----------|--|---------|--|--|
| Sumn Provides a s Networ | nary Dashbo summary of activity on the rk Threats | Dard (switch dashboard) e appliance Intrusion Events | Status | Geolocation | QoS | Device Management VPN NAT Site To Site QoS Remote Access Platform Settings Dynamic Access FlexConfig Troubleshooting Certificates Certificates | | VPN Site To Site Remote Access Dynamic Access Policy Troubleshooting | Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture |
| ▶ Тор (| Zero Trust Applicati | ons | | | - × | | | | Upgrade Threat Defense Upgrade Chassis Upgrade |

Toont het navigeren door de FMC GUI om naar de configuratie van het VPN-beleid voor externe toegang te gaan.

Bewerk het bestaande VPN-beleid voor externe toegang en maak een verbindingsprofiel met de naam 'DefaultRAGroup'

| þ | Firewall Management Center Devices / VPN / Remote Access | Overview | Analysis | Policies | Devices | Objects | Integration | | Deploy | ۹ (| • | 0 | admin \checkmark | ence SECURE |
|-----|---|----------|----------|----------|---------------|----------------------------|-------------|--|--------|-----|---|----|--------------------|-------------|
| | | | | | | | | | | | | | | Add |
| Nam | e | | | | Status | | | Last Modified | | | | | | |
| RAV | PN | | | | Targeting 1 d | devices on all targeted | | 2024-03-07 10:58:20 Modified by "admin" | | | | ۹. | / î | |
| | | | | | | | | | | | | | | |

Toont hoe u het beleid voor externe toegang VPN binnen de FMC UI kunt bewerken.

Bewerk de verbindingsprofielen met de namen 'DefaultWEBVPNGroup' en 'DefaultRAGroup'



Hier wordt getoond hoe de DefaultWEBVPNGgroup binnen de FMC UI moet worden bewerkt.

Navigeer naar het tabblad AAA en selecteer de vervolgkeuzelijst Verificatiemethode. Selecteer 'Alleen clientcertificaat' en selecteer Opslaan.

| Edit Connection Profile | | |
|---------------------------|--|---|
| Connection Profile:* | DefaultWEBVPNGroup | |
| Group Policy:* | DfltGrpPolicy + | |
| Client Address Assignment | AAA Aliases | |
| Authentication | | |
| Authentication Method: | Client Certificate Only - | |
| • | Enable multiple certificate authentication | |
| Map username from clier | nt certificate | |
| Authorization | | |
| Authorization Server: | | |
| | Allow connection only if user exists in authorization database | |
| Accounting | | |
| Accounting Server: | ▼ | |
| | | |
| | | |
| | | |
| | Cancel | е |

De verificatiemethode wijzigen in clientcertificaat alleen voor de DefaultWEBVPNGgroep binnen de FMC UI.

Bewerk de DefaultRAG groep en navigeer naar het tabblad AAA en selecteer de vervolgkeuzelijst Verificatiemethode. Selecteer 'Alleen clientcertificaat' en selecteer Opslaan.

| Edit Connection Profile | | |
|---------------------------|--|----|
| Connection Profile:* | DefaultRAGroup | |
| Group Policy:* | DfltGrpPolicy + | |
| Client Address Assignment | AAA Aliases | |
| Authentication | | |
| Authentication Method: | Client Certificate Only - | |
| | Enable multiple certificate authentication | |
| Map username from clie | nt certificate | |
| Authorization | | |
| Authorization Server: | ▼ | |
| | Allow connection only if user exists in authorization database | |
| Accounting | | |
| Accounting Server: | ▼ | |
| | | |
| | | |
| | | |
| | Cancel | ve |

De verificatiemethode wijzigen in clientcertificaat alleen voor de DefaultRAGgroup binnen de FMC UI.



Opmerking: de verificatiemethode kan ook een AAA-server met een sinkhole zijn. Als deze methode wordt gebruikt, is de AAA-serverconfiguratie nep en worden geen aanvragen daadwerkelijk verwerkt. Een VPN-pool moet ook worden gedefinieerd in het tabblad 'Clientadrestoewijzing' om de wijzigingen op te slaan.

Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel)

Dit is alleen nodig als u Hostscan / Secure Firewall postuur in uw omgeving heeft. Deze stap voorkomt dat aanvallers het resourcegebruik op de firewall vergroten, wat wordt veroorzaakt door het endpointscanproces. In het VCC wordt dit bereikt door een FlexConfig-object met de opdracht zonder CSD te maken om de functionaliteit voor endpointscannen uit te schakelen.

Navigeer naar objecten > Objectbeheer > FlexConfig-object > FlexConfig-object toevoegen.

| Firewall Manageme Objects / Object Managem | nt Center Overview Analysis Policies Devices Objects Integration | Deploy Q 🥩 🌣 🎯 admin 🗸 | resco SECURE | | | | | |
|--|--|---|----------------|--|--|--|--|--|
| > AAA Server > Access List > Address Pools Application Filters | FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices. | Add FlexConfig Object | | | | | | |
| AS Path | AS Path Description | | | | | | | |
| BFD Template Circhert Suite List | Anyconnect_route_titlering | | §/₹^ | | | | | |
| Community List | Default_DNS_Configure | Configure Default DNS with the help of TextObjects defaultDNS | 5 <u>6</u> q ⊒ | | | | | |
| DHCP IPv6 Pool | Default_Inspection_Protocot_Disable | Disable Default Inspection. | ¶a ⊂, | | | | | |
| Distinguished Name DNS Secure Group | Default_Inspection_Protocot_Enable | Enable Default Inspection. | ¶aq | | | | | |
| > External Attributes | DHCPv6_Prefx_Delegation_Configure | Configure one outside (PD client) and one inside interface (recip | ¶a ⊂ | | | | | |
| File List | DHCPv6_Prefx_Delegation_UnConfigure | Remove configuration of one outside (PD client) and one inside i | 5 a ⊂ ∋ | | | | | |
| FlexConfig ElexConfig Object | DNS_Configure | Configure DNS with the help of TextObjects dnsParameters and | F a ⊂ ≣ | | | | | |
| Text Object | DNS_UnConfigure | Remove the DNS configurations. | ¶aq ⊒ | | | | | |
| Geolocation | Eigrp_Configure | Configures eigrp. 1. Configures next hop. 2. configures auto-su | ¶a q ⊒ | | | | | |
| Interface Key Chain | Eigrp_interface_Configure | Configures interface parameters for eigrp. 1. Configures authent | ¶a Q ⊒ | | | | | |
| Network | Eigrp_UnConfigure | Clears eigrp configuration for an AS | Γ βα, ⊒ | | | | | |

Navigeren in de FMC UI om een FlexConfig-object te maken.

Geef het FlexConfig-object een naam en stel de implementatie in op Everytime met het type Add. Typ vervolgens de syntaxis precies zoals aangegeven op de afbeelding en sla het object op.

| Edit FlexConfig Object | | | | | | | 0 |
|---|----------------------|-----------------------|-----------|------------|--------------------|-------------|------|
| Name: Wtihout-CSD Description: Copy-pasting any rich text might info | troduce line breaks | s while generating CL | I. Please | verify the | CLI before deployr | ment. | |
| Insert 🔻 🔣 Deployment | Everytime | | • | Туре: | Append | • | |
| without-csd | n-attributes | - | | | | | |
| | D iana and an | B-fH-H-I | Prop | erty | 0 | B | |
| Name | Dimension | Default Value | (Туре | e:Name) | Override | Description | |
| | | No records to o | aisplay | | | | |
| | | | | | | | |
| | | | | | | Cancel | Save |

Een FlexConfig-object maken met 'zonder CSD'

Navigeer naar Apparaten > FlexConfig en klik vervolgens op het potlood om het FlexConfig-beleid

te bewerken.

| L Devices / IsoConfig | admin ~ admin SECURE |
|---|----------------------|
| | New Policy |
| FlexConfig Policy Status Last Modified | |
| Flex-Test Targeting 1 devices 2024-04-10 21:54:19 Out-of-cable on 1 largeted devices Modified by "admin" | 4 🖊 i |
| | |
| | |
| | |

Het FlexConfig-beleid binnen het VCC bewerken.

Bepaal de plaats van het voorwerp u van de Gebruiker bepaalde sectie creeerde. Selecteer vervolgens het pijltje om het toe te voegen aan de geselecteerde Toevoeging FlexConfiguraties. Selecteer ten slotte Opslaan om het FlexConfig-beleid op te slaan.

| Firewall Management Center Devices / Flexconfig Policy Editor | Overview | Analysis | Policies | Devices | Objects | Integration | | Deploy | | ° 0 | admin \sim | cisco SEC | |
|--|----------|---------------|------------|---------|-------------|-------------|--|--------------|--------|-----|--------------|-----------|-------|
| FlexConfig Enter Description | | | | | | | | nges Migrate | Config | | Config Poli | Save Car | s (1) |
| | n Selec | ted Prepend F | lexConfigs | | | | | | | | | | |
| Available FlexConfig C FlexConfig Object | = N | lame | | | Description | | | | | | | | |
| Vuser Defined | 1 | | | | | | | | | | | | |
| ¹ Anyconnect_route_filtering ¹ Keepout ¹ Ne_Keepout ² Without-CSD ✓ System Defined ² Default_DNS_Configure | | | | | | | | | | | | | |
| Default_Inspection_Protocol_Disable Default_Inspection_Protocol_Enable | - Calas | ted Assess 7 | au Canfina | | | | | | | | | | |
| 2 DHCPv6_Prefix_Delegation_Configure | 50100 | ted Append Fi | exconings | | | | | | | | | | |
| J DHCPv6_Prefix_Delegation_UnConfigure | = N | lame | | | Description | | | | | | | | |
| "? DNS_Configure | 1 1 | /tihout-CSD | | | | | | | | | | ٩. | |
| DNS_UnConfigure | | | | | | | | | | | | | |
| *? Eigrp_Configure | | | | | | | | | | | | | |
| P Finm Interface Configure | | | | | | | | | | | | | |

Hang het object FlexConfig aan het beleid voor FlexConfig.

Selecteer Beleidstoewijzingen en kies de FTD waarop u dit FlexConfig-beleid wilt toepassen en selecteer vervolgens OK. Selecteer nogmaals Opslaan als dit een nieuwe FlexConfig-toewijzing is en implementeer de wijzigingen. Controleer na implementatie of

| Firewall Management Center Devices / Flexcorify Policy Editor | Overview Anal | ysis Policies | Devices 0 | Objects Inte | egration | | | Deploy Q 🧬 🛱 😡 | admin ~ duto SECURE |
|--|----------------------|---|--------------------|---------------------|--------------------------------|---|--------|----------------|------------------------|
| FlexConfig Enter Description | | | | | | | | | Config Sava Cancel |
| Available FlexConfig C FlexConfig Object | Selected Prep | end FlexConfigs | Desc | cription | | | | | Policy Assignments (1) |
| V User Defined | | Targeted Devices Targeted Devices Select devices to t Available Devices Q. Search by nam FTD1 | swhich you want to | o apply this policy | y. Selected Devices FTD1 | Ŧ | | | |
| Default_Inspection_Protocol_Enable DHCPv6_Probs_Delegation_Configure DHCPv6_Probs_Delegation_UncConfigure DNS_Configure DNS_Configure DNS_Configure Egyp_Configure Egyp_Linterface_Configure Egyp_Linterface_Configure | Selected App Name | | | | | | Cancel | | Q. 🗑 |

Wijs het FlexConfig-beleid toe aan een FirePOWER-apparaat.

Voer de FTD CLI in en geef de opdracht show run tunnel-group voor de DefaultWEBVPNGGroup en DefaultRAGroup. Controleer of zonder-csd nu in de configuratie aanwezig is.

<#root>

FTD72#

show run tunnel-group DefaultRAGroup

tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate

without-csd

Groepsaliassen uitschakelen en Groep-URL's inschakelen

Navigeer naar een verbindingsprofiel en selecteer het tabblad 'Aliassen'. Schakel de groep-alias

uit of verwijder de groep-alias en klik op het plus pictogram om een URL alias toe te voegen.

| Edit Connection Profile | | | | | | | |
|--|----------|---|--|--|--|--|--|
| Connection Profile:* LDAP-TG | | | | | | | |
| Group Policy:* DfltGrpPolicy | • + | | | | | | |
| Edit Group Policy Client Address Assignment AAA Aliases | | | | | | | |
| Alias Names: | | | | | | | |
| Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display. | | | | | | | |
| | | + | | | | | |
| Name | Status | | | | | | |
| LDAP | Disabled | 1 | | | | | |
| | | | | | | | |
| URL Alias: | | | | | | | |
| Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile | | | | | | | |
| | | + | | | | | |
| URL | Status | | | | | | |
| | | | | | | | |

Schakel de optie voor groepsalias uit voor een tunnelgroep binnen de FMC UI.

Configureer een objectnaam voor de URL-alias en vul het FQDN- en/of IP-adres van de firewall voor de URL in, gevolgd door de naam waaraan u het verbindingsprofiel wilt koppelen. In dit voorbeeld kozen we voor 'aldap'. Hoe onduidelijker, hoe veiliger, omdat het minder waarschijnlijk is dat aanvallers de volledige URL raden, zelfs als ze uw FQDN hebben verkregen. Als u klaar bent, selecteert u Opslaan.



Een URL-aliassobject maken binnen de FMC UI.

Selecteer de URL-aliassen in de vervolgkeuzelijst, controleer het vakje Ingeschakeld en selecteer OK.



Zorg ervoor dat de URL-alias is ingeschakeld binnen de FMC UI.

Zorg ervoor dat de groep-alias is verwijderd of uitgeschakeld en controleer of uw URL-alias nu is ingeschakeld en selecteer Opslaan.

| Edit Connection Profile | | 0 |
|--|-----------------------------|-----------|
| Connection Profile:* LDAP-TG | | |
| Group Policy:* DfltGrpPolicy Edit Group Policy | • + | |
| Client Address Assignment AAA Aliases | | |
| Incoming users can choose an alias name upon first login. Alia on this device can be turned on or off for display. | ases from all connections c | onfigured |
| Name | Status | |
| LDAP | Disabled | /1 |
| LIDI Alias | | |
| Configure the list of URL alias which your endpoints can select | t on web access. If users o | hoose the |
| following URLs, system will automatically log them in via this | connection profile. | + |
| URL | Status | |
| LDAP-ALIAS (https://ftd1 com/aaaldap) | Enabled | 17 |
| | | • |
| | Cancel | Save |

De optie URL-alias inschakelen voor een tunnelgroep binnen de FMC UI.

Indien gewenst, kunnen URL aliassen ook worden gedrukt als deel van de XML. Dit wordt bereikt door XML te bewerken met de VPN Profile Editor of de ASA Profile Editor. Om dit te realiseren, navigeer naar het tabblad Serverlijst en zorg ervoor dat het veld Gebruikersgroep overeenkomt met de URL-aliassen van het verbindingsprofiel bij gebruik van SSL. Zorg er voor dat voor IKEv2 het veld Gebruikersgroep overeenkomt met de exacte naam van het verbindingsprofiel.

| Server List Entry X Server Load Balancing Servers SCEP Mobile Certificate Pinning Primary Server Connection Information Display Name (required) FTD1-SSL FQDN or IP A Der Group Maximum Auth Method During INE Negotiation EAP-AnyConnect V |
|---|
| Group LIPL IKE Identity (ICS gateway only) ftd1 |
| Move LD Move D Delete |

Het bewerken van het XML-profiel om een URL-alias voor SSL-verbindingen te hebben.

Toewijzing van certificaten

Navigeer naar het tabblad Geavanceerd binnen het VPN-beleid voor externe toegang. Kies een algemene instellingsoptie op basis van uw voorkeur. Selecteer Toewijzing toevoegen als u dit hebt geselecteerd.

| RAVPN Enter Description | | Yos have unswed changes Save Cancel Policy Assignments (1) |
|--|---|--|
| Connection Profile Access Inter | aces Advanced | Local Realm: None Dynamic Access Policy; None |
| Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries Custom Installer Transforms | General Settings for Connection Profile Mapping The device processes the policies in the order listed below until it finds a match Use group URL of group URL and Certificate Map match different Connection Profiles Use the configured rules to match a certificate Map match different Connection Profile Certificate to Connection Profile Mapping Clerificate to Connection Profile Mapping Clerif request is checked against each Certificate Map, associated Connection Profile will be used when rules are matched. If none of the Certificate Map is m Please provide at least one Certificate Mapping | witched, default connection profile will be chosen. |
| Localized Installer Transforms | Certificate Map Connection Profile | |
| Address Assignment Policy | No Records Found | |
| Caronicate Mapps Group Policies LDAP Attribute Mapping Load Balancing V IPaec Crypto Maps IKE Policy | | |
| IPsec/IKEv2 Parameters | Default Connection Profile: This Connection Profile: This Connection Profile will be applied orders none of the Contificate May's rule is matched. | · · · · · |

Navigeren naar het tabblad Geavanceerd binnen de FMC UI om een certificaatkaartobject te maken binnen de FMC UI.

Geef het object van de certificaattoewijzing een naam en selecteer Regel toevoegen. Definieer in deze regel de eigenschappen van het certificaat dat u wilt identificeren om de gebruiker aan een bepaald verbindingsprofiel toe te wijzen. Als u klaar bent, selecteert u OK en vervolgens selecteert u Opslaan.

| Add | Certificate Map | | | | 0 |
|----------------------------|---|------------------|----------|-----------|----------|
| Map Ce Mapp Confi | Name*: rtificate-Map-CN ping Rule igure the certificate ma | atching rule | | | Add Rule |
| # | Field | Component | Operator | Value | |
| 1 | Subject • | CN (Common Nam 🔻 | Equals 🔻 | customval | ue |
| | OK Cancel | | | | |
| | | | | Cance | Save |

Maak een certificaatkaart en voeg criteria toe voor de kaart binnen de FMC UI.

Selecteer in de vervolgkeuzelijst het object van de certificaatkaart en het verbindingsprofiel waaraan u de certificaatkaart wilt koppelen. Selecteer vervolgens OK.

| Add Connection Profile to Certificate Map | |
|---|--|
| Choose a Certificate Map and associate Connection Profiles to selected Certficate Map. | |
| Certificate Map Name*: | |
| Certificate-Map-CN + | |
| Connection Profile*: | |
| LDAP-TG 🔻 | |
| | |
| Cancel | |

Koppel het object van de certificaatkaart aan de gewenste tunnelgroep binnen de FMC UI.

Zorg ervoor dat het Default Connection Profile is geconfigureerd als DefaultWEBVPNGgroup, zodat als een gebruiker de mapping mislukt, deze wordt verzonden naar de DefaultWEBVPNGgroup. Als u klaar bent, selecteert u Opslaan en implementeert u de wijzigingen.

| RAVPN | | You h | we unsaved changes Save Cancel |
|---------------------------------|---|---|--------------------------------|
| Enter Description | | | |
| | | | Policy Assignments (1) |
| Connection Profile Access Inter | feen Advanced | Local Realm: None | Dynamic Access Policy: None |
| Connection Prolite Access meet | aces Advanced | | |
| Secure Client Images | General Settings for Connection Profile Mapping | | |
| Secure Client Customization | The device processes the policies in the order listed below until it finds a match | | |
| GUI Text and Messages | Use group URL if group URL and Certificate Map match different Connection Profiles | | |
| Icons and Images | Use the configured rules to match a certificate to a Connection Profile | | |
| Scripts | Certificate to Connection Profile Mapping | had. If sees of the Catificate Man is matched, default connection confis will be chosen | |
| Binaries | Cient request is checked against each Ceruncate wap, associated Connectorin Prome war or used when rules are made | neo. Il none or the Certificate wap is matched, delater connection prove was be endere. | Add Mansion |
| Custom Installer Transforms | | | Add Mapping |
| Localized Installer Transforms | Certificate Map | Connection Profile | |
| Address Assignment Policy | Certificate-Map-CN | LDAP-TG | 1 |
| Certificate Maps | | | |
| Group Policies | | | |
| LDAP Attribute Mapping | | | |
| Load Balancing | | | |
| v IPsec | | | |
| Crypto Maps | | | |
| IKE Policy | | | |
| IPsec/IKEv2 Parameters | Default Connection Profile: | | DefaultWEBVPNGroup * |
| | | | |

Verander het standaardverbindingsprofiel voor certificaatomzetting in DefaultWEBVPNGroup binnen de FMC UI.

IPsec-IKEv2

Selecteer het gewenste IPsec-IKEv2 verbindingsprofiel en navigeer om het groepsbeleid te

bewerken.

| Edit Connection Profil | e | |
|--------------------------|----------------|--|
| Connection Profile:* | IKEV2 | |
| Group Policy:* | IKEV2-IPSEC + | |
| Client Address Assignmer | it AAA Aliases | |

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

| IP Address Range | |
|------------------------|--|
| 10.50.50.1-10.50.50.6 | /1 |
| | |
| | |
| | + |
| DHCP Server IP Address | |
| | |
| | |
| Cancel | Save |
| | IP Address Range 10.50.50.1-10.50.50.6 DHCP Server IP Address Cancel |

Bewerk een groepsbeleid binnen de FMC UI.

Ga op het tabblad Algemeen naar het gedeelte VPN-protocollen en controleer of het vakje IPsec-IKEv2 is ingeschakeld.

| Edit Group Policy | | |
|--|---|----|
| Name:* IKEV2-IPSEC Description: | | |
| General Secure | Client Advanced | |
| VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling | VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling more must be configured for users to connect over a VPN tunnel. □ SSL ✓ IPsec-IKEv2 | te |

Schakel IPsec-IKEv2 in binnen een groepsbeleid in de FMC UI.

In de VPN Profile Editor of ASA Profile Editor navigeer je naar het tabblad Server List. De naam van de gebruikersgroep MOET exact overeenkomen met de naam van het verbindingsprofiel in de firewall. In dit voorbeeld, IKEV2 was de verbinding profiel / Gebruikersgroep naam. Het primaire protocol wordt geconfigureerd als IPsec. De 'Display Name' in wordt weergegeven aan de gebruiker in de Secure Client UI wanneer een verbinding met dit verbindingsprofiel wordt gemaakt.

| Server List Entry | × |
|---|--|
| Server Load Balancing Servers SCEP Mobile Certifica | ate Pinning |
| Primary Server Display Name (required) FTD1-IPSEC FQDN or IP A User Group ftd1com / IKEV2 Group URL | Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only) |
| Backup Servers Host Address | Add Move Up Move D Delete |
| ОК | Cancel |

Bewerk het XML-profiel zodat het primaire protocol IPsec is, en de gebruikersgroep overeenkomt met de naam van het verbindingsprofiel.



Waarschuwing: er is een SSL-verbinding nodig om XML-profielen vanuit de firewall naar de client te duwen. Wanneer alleen IKEV2-IPsec wordt gebruikt, moeten de XML-profielen via een out-of-band methode naar de clients worden gedrukt.

Nadat het XML-profiel naar de client is gedrukt, gebruikt Secure Client de gebruikersgroep van het XML-profiel om verbinding te maken met het IKEV2-IPsec-verbindingsprofiel.

| 🕱 Cisco Secur | e Client | _ | | × |
|---------------|---|---|---------|---------|
| | AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC | ~ | Connect | _ |
| Cisco Se | cure Client FTD1-IPSEC | | × | altalte |
| Us Pa | ername: nroche ssword: | | | |
| | | 1 | | |

Beveiligde client-UI-weergave van de poging tot verbinding met IPsec-IKEv2 RAVPN.

ASA-configuratievoorbeelden

AAA-verificatie uitschakelen in de standaard-WEBVPNG-groep en DefaultRAGroupverbindingsprofielen

Voer de sectie webvpn-attributen voor de tunnelgroep DefaultWEBVPNGroup in en specificeer de verificatie als op certificaat gebaseerd. Herhaal dit proces voor de DefaultRAG groep. Gebruikers die landen op deze standaard verbindingsprofielen worden gedwongen om een certificaat voor authenticatie voor te stellen en krijgen niet de kans om gebruikersnaam en wachtwoord referenties in te voeren.

Hostscan/Secure Firewall postuur uitschakelen in de DefaultWEBVPNGroup en DefaultRAGroup (optioneel)

Dit is alleen nodig als u Hostscan / Secure Firewall postuur in uw omgeving heeft. Deze stap voorkomt dat aanvallers het resourcegebruik op de firewall vergroten, wat wordt veroorzaakt door het endpointscanproces. Voer de sectie webvpn-attributen in voor de profielen DefaultWEBVPNGroup en DefaultRAGroup en connection en implementeer zonder-csd om de functionaliteit voor endpointscannen uit te schakelen.

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

Groepsaliassen uitschakelen en Groep-URL's inschakelen

Voer de tunnelgroep(en) in waarmee gebruikers verbinding maken. Als er een bestaand groepsalias is, schakelt u het uit of verwijdert u het. In dit voorbeeld is het uitgeschakeld. Zodra dat is voltooid, maakt u een groep-url met behulp van het FQDN- of IP-adres van de RAVPN-afsluitinterface. De naam aan het einde van de groep-url moet onduidelijk zijn. Vermijd gemeenschappelijke waarden zoals VPN, AAA, RADIUS, LDAP, aangezien deze het voor aanvallers gemakkelijker maken om de volledige URL te raden als zij FQDN verkrijgen. Gebruik in plaats daarvan intern significante namen die u helpen de tunnelgroep te identificeren.

ASA# configure terminal ASA(config)# tunnel-group NAME webvpn-attributes ASA(config-tunnel-webvpn)# group-alias NAME disable ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable

Toewijzing van certificaten

Van globale configuratiewijze, creeer een certificaatkaart en wijs het een naam en een opeenvolgingsaantal toe. Definieer vervolgens een regel die gebruikers moeten aanpassen om de afbeelding te gebruiken. In dit voorbeeld zouden gebruikers moeten voldoen aan de criteria van een algemene naamwaarde die gelijk is aan "customvalue". Voer vervolgens de webvpnconfiguratie in en pas de certificaatkaart toe op de gewenste tunnelgroep. Voer na voltooiing de DefaultWEBVPNG-groep in en maak van deze tunnelgroep de standaard voor gebruikers die de certificaattoewijzing niet doorstaan. Als gebruikers falen in de mapping, worden ze doorgestuurd naar de DefaultWEBVPNG groep. Terwijl de DefaultWEBVPNG groep is geconfigureerd met certificaatverificatie, hebben gebruikers niet de optie om gebruikersnaam of wachtwoordreferenties door te geven.

ASA(config)# crypto ca certificate map NAME 1 ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

```
ASA(config)# webvpn
ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME
```

```
ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes
ASA(config-tunnel-webvpn)# tunnel-group-map default-group
```

IPsec-IKEv2

Van globale configuratiewijze, kunt u een bestaand groepsbeleid bewerken of nieuwe creëren en de attributen voor dat groepsbeleid invoeren. Zodra u in de attributensectie bent, laat IKEv2 als enig VPN tunnelprotocol toe. Zorg ervoor dat dit groepsbeleid is gekoppeld aan een tunnelgroep die wordt gebruikt voor IPsec-IKEV2 VPN-verbindingen voor externe toegang. Gelijkaardig aan de stappen van het FMC, moet u het profiel van XML via de Redacteur van het Profiel van VPN of de ASA Redacteur van het Profiel bewerken en het gebied van de Gebruikersgroep veranderen om de naam van de tunnelgroep op ASA aan te passen, en het protocol veranderen in IPsec.

```
ASA# configure terminal
ASA(config)# group-policy GP-NAME internal
ASA(config)# group-policy GP-NAME attributes
ASA(config-group-policy)# vpn-tunnel-protocol ikev2
```

```
ASA(config)# tunnel-group TG-NAME general-attributes
ASA(config-tunnel-general)# default-group-policy GP-NAME
```

In de VPN Profile Editor of ASA Profile Editor navigeer je naar het tabblad Server List. De naam van de gebruikersgroep MOET exact overeenkomen met de naam van het verbindingsprofiel in de firewall. Het primaire protocol wordt geconfigureerd als IPsec. De naam van de weergave wordt aan de gebruiker in de Beveiligde client-gebruikersinterface getoond wanneer een verbinding met dit verbindingsprofiel wordt gemaakt.

| Server List Entry | × |
|---|---|
| Server Load Balancing Servers SCEP Mobile Certific | cate Pinning |
| Primary Server Display Name (required) ASA-IPsec FQDN or IP A FQDN FQDN FQDN FQDN FQDN FQDN FQDN FQDN | Connection Information Primary Protocol IPsec ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect IKE Identity (IOS gateway only) |
| EQDN/TG-NAME Backup Servers Host Address | Add Move Up Move D Delete |
| ОК | Cancel |

Bewerk het XML-profiel zodat de primaire protocolnaam IPsec is en de gebruikersnaam voor de gebruikersgroep overeenkomt met de tunnelgroepnaam van de ASA voor IPsec-IKEv2 RAVPN-verbindingen.



Waarschuwing: er is een SSL-verbinding nodig om XML-profielen vanuit de firewall naar de client te duwen. Wanneer alleen IKEV2-IPsec wordt gebruikt, moeten de XML-profielen via een out-of-band methode naar de clients worden gedrukt.

Conclusie

Samenvattend, het doel van de verhardende praktijken in dit document is legitieme gebruikers in kaart te brengen aan aangepaste verbindingsprofielen terwijl de aanvallers worden gedwongen aan de DefaultWEBVPNGroup en de DefaultRAGroup. In een geoptimaliseerde configuratie hebben de twee standaardverbindingsprofielen geen legitieme aangepaste AAA-serverconfiguratie. Bovendien voorkomt de verwijdering van groepsaliassen dat aanvallers eenvoudig aangepaste verbindingsprofielen kunnen identificeren door de drop-down zichtbaarheid te verwijderen bij het navigeren naar de FQDN of het openbare IP-adres van de firewall.

Gerelateerde informatie

- Cisco technische ondersteuning en downloads
- Aanvallen met wachtwoordspeling
- Onbevoegde toegangskwetsbaarheid september 2023
- ASA-configuratiehandleidingen
- Configuratiehandleidingen voor FMC/FDM

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.