Desative o tempo limite ocioso de VPN site a site do FTD com políticas FlexConfig

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar Configurar Configurar a política FlexConfig e o objeto FlexConfig Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como modificar o atributo **vpn-idle-timeout** de uma VPN com Políticas FlexConfig no Cisco Firepower Management Center (FMC) para evitar o tempo de inatividade do túnel devido ao tempo limite de inatividade ou ociosidade.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- FMC
- Políticas FlexConfig
- Topologias de VPN site a site

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- FMCv 6.5.0.4 (build 57)
- FTDv 6.4.0.10 (build 95)

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Tanto o Internet Key Exchange versão 1 (IKEv1) como o Internet Key Exchange versão 2 (IKEv2) Policy Based (mapa de criptografia) VPNs site a site são túneis sob demanda. Por padrão, o FTD encerra a conexão VPN se não houver nenhuma atividade de comunicação no túnel em um determinado período chamado **vpn-idle-timeout**. Esse temporizador é definido como 30 minutos por padrão.

Configurar

Configurar a política FlexConfig e o objeto FlexConfig

Etapa 1. Em **Dispositivos > FlexConfig** crie uma nova política FlexConfig (se ainda não existir) e a anexe ao FTD onde a VPN de site a site está configurada.

| cisco Firepower Manag | gement C × + | | - | - 🗆 × |
|--|----------------------------------|--------------------------|--------------|-----------------|
| $\leftarrow \rightarrow$ C \textcircled{O} O | https://10.31.124.31:6005/ | ddd/#Flexc 90% 🏠 | ☆ 🛛 🖬 | \$** @ ≡ |
| Getting Started 💮 New Tab | 🖉 BEMS 🏾 🎯 Identity Services Er | gine 號 Next Generation W | /eb >>> [] | Other Bookmarks |
| Overview Analysis Policie | es Devices Objects AMP | Intelligence Deploy | / 🔍 System I | Help 🔻 admin 🔻 |
| Device Management NAT | VPN QoS Platform Setti | ngs FlexConfig Cer | rtificates | |
| | | | | 💿 New Policy |
| FlexConfig Policy | Status | Last Mod | lified | |
| New Policy | | | ŕ | |
| Description: | :xconiig_FTD_B | | | |
| Targeted Devices | | | | D 0 |
| Available Devices | · value Add to Policy | Selected Devices | Cancel | |
| | | | | |
| Last login on Monday, 2021-07-05 at 16 | 5:03:21 PM from 10.24.67.117 How | То | | uluulu cisco |

| tisco Firepower Management C × + | | | - 🗆 × |
|---|---|--|-------------------|
| \leftarrow \rightarrow C \textcircled{a} \bigcirc \textcircled{b} https://10. | 31.124.31:6005/ddd/#Flexc 90% | 5 ☆ ☆ ♡ . | |
| 💮 Getting Started 💮 New Tab 🖉 BEMS 🥘 🛛 | dentity Services Engine 🛯 👹 Next Ge | neration Web >>> | C Other Bookmarks |
| Overview Analysis Policies Devices C | Dbjects AMP Intelligence | Deploy 🧕 System | Help 🔻 admin 🔻 |
| Device Management NAT VPN ▼ QoS | Platform Settings FlexConf | ig Certificates | |
| | | | 📀 New Policy |
| FlexConfig Policy | Status | Last Modified | |
| FlexConfig_FTD_B | Targeting 1 devices Up-to-date on all targeted devices | 2021-06-15 17:21:38 Modified by "admin" | la 🦉 🔁 |

Etapa 2. Dentro dessa política, crie um objeto FlexConfig da seguinte maneira:

Nome: S2S_Idle_TimeOut Implantação: Sempre Digite: Acrescentar

group-policy .DefaultS2SGroupPolicy atributos vpn-idle-timeout none

| tite Cisco Firepower Management C × + | | - 🗆 X |
|--|--|---------------------------------------|
| \leftarrow \rightarrow C \textcircled{a} \bigcirc \textcircled{b} https://10.3 | 31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C29 | 88 90% ☆ 途 🛛 🖶 🗰 💿 🚍 |
| 🕀 Getting Started 🕀 New Tab 🥖 BEMS 🧐 Identity | / Services Engine 📸 Next Generation Web 📷 Regex Tester | and Deb 🍥 Mi vacuna 🗋 Other Bookmarks |
| Overview Analysis Policies Devices Object | ts AMP Intelligence | Deploy 🧕 System Help 🔻 admin 🔻 |
| Device Management NAT VPN VPN QoS Pla | tform Settings FlexConfig Certificates | |
| FlexConfig_FTD_B | | Preview Config 🔄 Save 🛛 🔀 Cancel |
| Enter Description | | Policy Assignments (1) |
| Available FlexConfig C SlexConfig Object | Selected Prepend FlexConfigs | |
| | # Name | Description |
| | | |
| User Defined | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Selected Append FlexConfigs | |
| 4 🧭 System Defined | # Name | Description |
| Default_DNS_Configure | | |
| Default_Inspection_Protocol_Disable | | |
| DHCPy6 Prefix Delegation Configure | | |
| DHCPv6_Prefix_Delegation_UnConfigure | | |
| DNS_Configure | | |
| DNS_UnConfigure | | |
| Eigrp_Configure | | |
| Eigrp_Interface_Configure | | |
| Eigrp_Unconfigure_All | | |
| | | |
| | | |
| Last login on Monday, 2021-07-05 at 16:03:21 PM from 10.24.67.11 | 7 How To | |

| (| cisco Firepowe | er Manage | ement C × | cisco C | isco Firepo | ower Man | agement⊂× | + | | | | | | | | - | - | | × |
|--------------|-----------------------------------|------------------|---------------|--------------------|--------------|-------------------|----------------|--------------|------------|-------------|------------|----------|-----------|------------|------------|------|---------|-----------|-------|
| \leftarrow | \rightarrow C C | | | https://1 | 10.31.124 | 4.31 :6005 | /ddd/#Flexc | onfigPolicy | yEditor;u | uid=000C | 2988- | 90% | ŝ | 公 | ${\times}$ | | 4110 | ms | ≡ |
| 🕀 Ge | etting Started 🕀 N | New Tab | @ BEMS | 🇐 Ider | ntity Servio | ces Engine | e 🎎 Next Ge | eneration W | eb tool | Regex Tes | ster and D |)eb (| 🌖 Mi vacu | ina | | C |] Other | r Book | marks |
| Over | view Analysis | Policies | Devic | es Obj | jects | AMP Ir | ntelligence | | | | | | Deploy | 0 1 | System | Hel | p₹ra | dmin | • ^ |
| Devic | e Add FlexConf | iig Obje | ct | | | | | | | | | | | | | | ? | × | |
| Enter (| Name: | S2S_I | dle_TimeOu | it | | | | | | | | | | | | | | | |
| Ava | Description: | | | | | | | | | | | | | | | | | nt | ; (1) |
| | A Copy-pag | ting any ri | ich text mig | ht introdu | ce line bre | ake while (| generating CLI | Diesse veri | fy the CLI | hefore deni | ovment | | | | | | | J. | |
| 4 | Insert - | | | | ce inte bre | and mine | generating cer | . ricuse ven | ly the cer | | De | ployment | : Everyt | ime 🗸 | Type: | Appe | nd v | 1 | |
| | group-pol <u>vpn-idle</u> | licy . a-time | Default | tS2SGr | oupPol | icy at | tributes |] | | | | | | | | | | 5 | |
| | Variables Name | | | | Dimens | ion | Default Val | lue | Propert | ty (Type | Overrid | le | Descri | iption | | | | | |
| | | | | | | | No rea | cords to o | display | | | | | | | | | | |
| Last lo | gi r on Honday, 2022 o | | 0.912.1.11.1. | /// <u>1912-99</u> | ,,,,,, | | | How To | | | | | | Sa | ave | 6 | Cancel | | |
| < | | | | | | | | | | | | | | | | | | eisee | |

e **Salve**-o.

Etapa 3. No painel esquerdo, procure-o e arraste-o para o painel direito com o botão >.

| | cisco Firepower Manag | gement C × | + | | | | | | | | | | | - | | × |
|------|---|--------------------|---------|----------------|-----------|---------------|-------------|--------------|-------------|--------|---------|-------------|--------|-------------|----------|--------|
| ~ | → C ŵ | O 🔓 http | s://10 |).31.124.31: | 6005/dd | d/#Flexconf | igPolicyEdi | tor;uuid=000 | C2988- | 90% | 숪 | 岔 | | | . 💿 | = |
| 0 | Setting Started A New Tab | | Ident | ity Services F | ngine 🐙 | Next Gener | ation Web | Regev Te | ester and I | Deb | A Mi v | acupa | | | ther Bor | kmarks |
| | | Q DEMO | | | ingine un | a riext ocher | | neger i | coter and t | | | acuna | | | | - |
| Ove | erview Analysis Policie | es Devices | Obje | ects AMP | P Intell | igence | | | | | D | eploy | 1 Syst | tem Help | v ad | min ▼ |
| Dev | ice Management NAT | VPN VQ05 | ; P | latform Sett | tings | FlexConfig | Certifica | tes | | | | | | | | |
| Fle | xConfig_FTD_B | | | | | | | Y | ou have ur | nsaved | changes | Preview C | onfig | 😑 Save | 8 | Cancel |
| Ente | Description | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | 1 | 🖳 Policy A: | signmen | ts (1) |
| A | vailable FlexConfig 🕏 | FlexConfig Ol | oject | | Selected | d Prepend F | lexConfigs | | | | | | | | | |
| | | | × | # | | | Name | | | | [| Description | | | | |
| | | | | | | | | | | | | | | | | |
| | 4 🥩 User Defined | | ^ | | | | | | | | | | | | | |
| | aaa-server-map | | | | | | | | | | | | | | | |
| | disable-am | | | | | | | | | | | | | | | |
| | EEM_script_PeriodicLo | gOffAnyconnect | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | Idap-attribute-map | | | | | | | | | | | | | | | |
| | Management-access | | | | | | | | | | | | | | | |
| | MAT-T-Dicable | igarciam | | | | | | | | | | | | | | |
| l Ir | S25 idle timeout | | | | | | | | | | | | | | | |
| | | | | > | Selected | d Append F | exConfias | | | | | | | | | |
| | VPN-filter | | | | | | | | | | | | | | | |
| | 4 🧔 System Defined | | | * | | | Name | | | | I. | Description | | | | |
| | Default_DNS_Configur | e | | | | | | | | | | | | | | |
| | Default_Inspection_Pr | otocol_Disable | | | | | | | | | | | | | | |
| | Default_Inspection_Provide the section_Provide the section_Provide the section_Provide the section of the se | otocol_Enable | | | | | | | | | | | | | | |
| | DHCPv6_Prefix_Delega | ation_Configure | | | | | | | | | | | | | | |
| | DHCPv6_Prefix_Delega | ation_UnConfigure | | | | | | | | | | | | | | |
| | DNS_Configure | | | | | | | | | | | | | | | |
| | DNS_UnConfigure | | | | | | | | | | | | | | | |
| | Eigrp_Configure | | | | | | | | | | | | | | | |
| | Eigrp_Interface_Config | jure | | | | | | | | | | | | | | |
| | 📄 Eigrp_UnConfigure | | ~ | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | | | | | | _ | _ | | | | | | | | | |
| Last | login on Monday, 2021-07-05 at 16 | 5:03:21 PM from 10 | .24.67. | 117 | | | low To | | | | | | | | 1 | isco |

| | cisco Firepower Manag | gement C × | + | | | | | | | | | | | - | | × |
|--------|---------------------------------|--------------------|----------|-------------|----------|-----------------|---------------|---------------|------------|---------|--------|-------------|-------|------------|------------|----------------|
| ~ | → C ଲ | | os://10 | .31.124.31 | 1:6005/0 | ddd/#Flexconf | fiaPolicvEdit | or:uuid=0000 | C2988- | 90% | \$ | 岔 | | | ÷• 💿 | = |
| 0 | etting Started @ New Tab | | Ident | ty Services | Engine | the Next Gener | ration Web | Pagay Ta | stor and D | leb | Mi v | - | | | ther Roo | kmarks |
| | etting started @ New lab | ELIVIS | iuent | ty services | Engine | asto Next Gener | ation web | DOLS REGEX TE | ster and L | /eb | | acuna | | | | KINGINS |
| Ove | rview Analysis Policie | es Devices | Obje | cts AM | 1P Int | elligence | | | | | D | eploy 🛛 🧕 🧕 | Syst | tem Helj | o∙r ad | min 🔻 |
| Devi | ce Management NAT | VPN VOS | S P | latform Se | ttings | FlexConfig | Certificat | es | | | | | | | _ | |
| Fle | xConfig_FTD_B | | | | | | | Yo | ou have un | saved o | hanges | Preview C | onfig | 📄 Save | 8 0 | Cancel |
| Enter | Description | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | 🖳 Policy A | ssignmen | ts (1) |
| A | ailable FlexConfig 🖒 | FlexConfig Ol | bject | T | Selec | ted Prepend I | lexConfigs | | | | | | | | | |
| | | | × | | # | | Name | | | | D | escription | | | | |
| | | | | | | | | | | | | | | | | _ |
| | User Defined | | ^ | | | | | | | | | | | | | |
| | aaa-server-map | | | | | | | | | | | | | | | |
| | disable-am | -0.64 | | | | | | | | | | | | | | |
| | EEM_script_PeriodicLo | gOffAnyconnect | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| | Management accord | | | | | | | | | | | | | | | |
| | management-access | aarciam | | | | | | | | | | | | | | |
| | NAT-T-Disable | garciam | | | | | | | | | | | | | | |
| | S2S_idle_timeout | | | | | | | | | | | | | | | |
| | test | | | | Selec | ted Append F | lexConfigs | | | | | | | | | |
| | 📃 VPN-filter | | | | # | | Name | | | | C | escription | | | | |
| | 🛿 🣁 System Defined | | | Г | 1 | \$25 i | dle timeout | | | | | | | | | - |
| | Default_DNS_Configur | e | | | * | 525_1 | die_diffeode | | | | | | | | ~ | |
| | Default_Inspection_Pr | otocol_Disable | | | | | | | | | | | | | | |
| | Default_Inspection_Pr | otocol_Enable | | | | | | | | | | | | | | |
| | DHCPv6_Prefix_Delega | ation_Configure | | | | | | | | | | | | | | |
| | DHCPV6_Prefix_Delega | ation_UnConfigure | e | | | | | | | | | | | | | |
| | DNS_Configure | | | | | | | | | | | | | | | |
| | Eigen Configure | | | | | | | | | | | | | | | |
| | Eigrp_configure | oure | | | | | | | | | | | | | | |
| | Eigrp_Internate_coning | goi e | ~ | | | | | | | | | | | | | |
| | cigrp_oncomgure | | - | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |
| Last I | ogin on Monday, 2021-07-05 at 1 | 6:03:21 PM from 10 |).24.67. | 117 | | | low To | | | | | | | | ۱، c | lıılı. Isco |

Salve as alterações e implemente.

Etapa 3.1 (Opcional) Como etapa intermediária, depois que as alterações de configuração tiverem sido salvas, você poderá escolher **Preview Config** para garantir que os comandos FlexConfig estejam prontos para serem enviados no final da configuração.

| the Cisco Firepower Manag | ement $\subset \times$ define Cisco Firepower Management $\subset \times$ + | | - 🗆 × |
|--|---|----------------|------------------------|
| \leftarrow \rightarrow C \textcircled{a} | ♥ 🏠 https://10.31.124.31:6005/ddd/#FlexconfigPolicyEditor;uuid=000C2988- 90% 🗹 | ☆ 🖄 🖂 | . 4+• 💿 = |
| 💮 Getting Started 🛛 🕀 New Tab | 🖉 BEMS 🧐 Identity Services Engine 🗰 Next Generation Web 🧮 Regex Tester and Deb 🥘 | 👂 Mi vacuna | C Other Bookmarks |
| Overview Analysis Policie | s Devices Objects AMP Intelligence | Deploy 02 Sys | stem Help 🔻 admin 🔻 |
| Device Management NAT | VPN VPN QoS Platform Settings FlexConfig Certificates | | |
| FlexConfig_FTD_B | | Preview Config | Save Sancel |
| Enter Description Prev | iew FlexConfig | ? × | Delicy Assignments (1) |
| S | elect Device: FTDv_B | • | Policy Assignments (1) |
| Available FlexConfig | | | |
| User Defined aaa-server-mar; disable-am EEM_script_Per LDAP Idap-attribute-n Management-a; management-a; NAT-T-Disable S25_Idle_Time() test VPN-filter System Defined Default_Inspect Default_Inspect DHCPv6_Prefix, DHCPv6_Prefix, DHCPv6_Prefix, DNS_COnfigure Eigrp_UnConfigure | <pre>ging list MANAGER_VPN_EVENT_LIST level debugging class webro gging list MANAGER_VPN_EVENT_LIST level debugging class sev gging list MANAGER_VPN_EVENT_LIST level debugging class sup gging list MANAGER_VPN_EVENT_LIST level debugging class up logging FMC MANAGER_VPN_EVENT_LIST</pre> | Close | •.3 |
| Last login on Monday, 2021-07-05 at 16 | 103:21 PM from 10.24.67.117 How To | | սիսիս |

Verificar

Quando a implantação estiver concluída, você poderá executar esse comando no LINA (> system support diagnostic-cli) para confirmar se a nova configuração está lá:

firepower# show running-config group-policy .DefaultS2SGroupPolicy
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout none <<<----<omitted output>

Caution: Lembre-se de que essa alteração afeta todas as VPNs S2S no FTD. NÃO é uma configuração por túnel, mas global.

Mesmo que a configuração esteja lá, o túnel ativo precisa ser devolvido (**clear crypto ipsec sa peer** <*Remote_Peer_IP_Address>*) para que a alteração tenha efeito quando o túnel for estabelecido novamente. Você pode confirmar se a alteração está em vigor com este comando:

```
Connection : X.X.X.X
Index : 7 IP Addr : X.X.X.X
Protocol : IKEv1 IPsec
Encryption : IKEv1: (1)AES256 IPsec: (1)AES256
Hashing : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 400 Bytes Rx : 400
Login Time : 22:06:56 UTC Tue Jun 15 2021
Duration : 0h:18m:00s
Tunnel Zone : 0
IKEv1 Tunnels: 1
IPsec Tunnels: 1
IKEv1:
Tunnel ID : 7.1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Main Auth Mode : preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 85319 Seconds
D/H Group : 5
Filter Name :
IPsec:
Tunnel ID : 7.2
Local Addr : A.A.A.A/255.255.255.255/0/0
Remote Addr : B.B.B.B/255.255.255.128/0/0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 27719 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes <<<<<-----
Bytes Tx : 400 Bytes Rx : 400
Pkts Tx : 4 Pkts Rx : 4
```

O contador *de tempo ocioso limite* deve ser definido como 0 minutos em vez de 30 minutos e a VPN deve permanecer ativa independentemente da atividade/tráfego sendo executado sobre ela.

Note: No momento da escrita, existe um bug de aprimoramento para integrar a capacidade de modificar essa configuração diretamente no FMC sem a necessidade do Flexconfig. Consulte o bug da Cisco ID <u>CSCvr82274</u> - ENH: torne o vpn-idle-timeout configurável

Troubleshoot

No momento, não há informações específicas disponíveis para solucionar problemas.

Informações Relacionadas

- Guia de Configuração do Firepower Management Center, Versão 7.0 Capítulo: Políticas FlexConfig para Firepower Threat Defense
- Guia de Configuração do Firepower Management Center, Versão 7.0 Capítulo: VPNs de site a site para Firepower Threat Defense
- Suporte Técnico e Documentação Cisco Systems