Ativar recursos de segurança usando grupos de configuração para SDWAN

Contents

Introdução

Este documento descreve a configuração de NGFW, filtragem de URL, AMP e IPS/IDS por meio de grupos de configuração, incluindo instruções para o registro unificado.

Pré-requisitos

Viabilize a visibilidade de fluxo e de aplicativos

Se você estiver usando Grupos de política para definir políticas :

- Selecione Grupo de política e, em seguida, selecione Prioridade de aplicativo e SLA.
- Selecione Adicionar novo
- Clique em Configurações adicionais e ative a visibilidade do aplicativo e do fluxo

Se você estiver usando a política legada

- Selecione um perfil do complemento Cli no grupo de configuração e adicione estes comandos

```
policy
app-visibility
flow-visibility
```

Certifique-se de estar em conformidade com os pré-requisitos para os recursos, conforme indicado aqui https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/url-filtering.html

```
Note: If you are using the legacy policy along with Configuration groups :

Select Configuration and Click Security
Click Custom Options and select Policies/Profiles and then access these features to enable
```

Este documento concentra-se nos recursos a serem ativados usando grupos de políticas

Firewall de próxima geração (NGFW)

Para ativar o NGFW, execute as etapas mencionadas:

- Selecione o grupo de políticas, clique em NGFW e clique em Adicionar política de NGFW
- Dê um nome de política e clique em Avançar
- Selecionar grupo de configuração para associar à política de NGFW
- Adicione as regras e clique em Avançar
- Crie sua política de NGFW

Para habilitar o registro em log, edite a política de NGFW, selecione configurações adicionais e ative o registro em log unificado

Filtragem de URL

Para ativar a filtragem de URL para versões anteriores a 20.18:

- Selecione Configuration on UI (Configuração na interface do usuário), Policy group (Grupo de políticas) e clique em Groups of Interest (Grupos de interesses)
- Selecione Segurança e expanda Perfis

Para habilitar a filtragem de url para as versões 20.18 e posteriores:

- Selecione Configuration on UI e, em seguida, Policy group e, em seguida, clique em Objects and Profiles
- Selecionar perfis de segurança

Selecione adicionar filtragem de url, insira os detalhes e clique em salvar

Advanced malware protection (AMP)

Para ativar o AMP para versões anteriores a 20.18:

- Selecione Configuration on UI (Configuração na interface do usuário), Policy group (Grupo de políticas) e clique em Groups of Interest (Grupos de interesses)
- Selecione Segurança e expanda Perfis

Para ativar o AMP para as versões 20.18 e posteriores:

- Selecione Configuration on UI e, em seguida, Policy group e, em seguida, clique em Objects and Profiles
- Selecionar perfis de segurança

Selecione Proteção avançada contra malware e clique em Adicionar proteção avançada contra malware

Adicione os detalhes e clique em salvar

Sistema de prevenção contra invasões (IPS)/Detecção de prevenção contra invasões (IDS)

Para ativar o IPS/IDS para versões anteriores a 20.18:

- Selecione Configuration on UI (Configuração na interface do usuário), Policy group (Grupo de políticas) e clique em Groups of Interest (Grupos de interesses)
- Selecione Segurança e expanda Perfis

Para habilitar o IPS/IDS para as versões 20.18 e posteriores:

- Selecione Configuration on UI e, em seguida, Policy group e, em seguida, clique em Objects and Profiles
- Selecionar perfis de segurança

Selecione Prevenção de intrusão e clique em Adicionar prevenção de intrusão

Adicione os detalhes e clique em salvar

Criar Perfil de Inspeção Avançado (AIP)

Para ativar o AIP para versões anteriores a 20.18:

- Selecione Configuration on UI (Configuração na interface do usuário), Policy group (Grupo de políticas) e clique em Groups of Interest (Grupos de interesses)
- Selecione Segurança e expanda Perfis

Para habilitar o AIP para as versões 20.18 e posteriores:

- Selecione Configuration on UI e, em seguida, Policy group e, em seguida, clique em Objects and Profiles
- Selecionar perfis de segurança

Selecione Perfil de Inspeção Avançado e clique em Adicionar Perfil de Inspeção Avançado

- Insira os nomes de filtragem AMP/IPS/Url criados nas etapas anteriores e clique em salvar

Associação de AIP a NGFW

- Selecione Configuração, Grupos de políticas e clique em NGFW
- Edite a política de NGFW criada anteriormente
- Para as regras de NGFW criadas anteriormente, edite e associe o perfil AIP criado anteriormente e clique em salvar

Ulogging

Para efetuar log, ative o recurso no roteador através do grupo de configuração usando o complemento cli

```
policy
ip visibility features
ulogging enable

parameter-map type inspect-global
log dropped-packets
log flow-export fnf
log flow
!
utd engine standard unified-policy
utd global
flow-logging all
```

Verificação

```
show  flow monitor sdwan-flow-monitor cache

IPV4 SOURCE ADDRESS:                            10.100.10.75
IPV4 DESTINATION ADDRESS:                       10.10.10.25
TRNS SOURCE PORT:                               53
TRNS DESTINATION PORT:                          34796
IP VPN ID:                                      10
IP PROTOCOL:                                    17
tcp flags:                                      0x00
interface input:                                Gi2
interface output:                               Gi3
flow cts source group tag:                      0
flow cts destination group tag:                 0
counter bytes long:                             125
counter packets long:                           1
timestamp abs first:                            14:59:47.613
timestamp abs last:                             14:59:47.613
flow end reason:                                Not determined
connection initiator:                           Reverse initiator
interface overlay session id input:             10
interface overlay session id output:            0
connection connection id long:                  0x000000000050D9CC
drop cause id:                                  0
counter bytes drop long:                        0
sdwan sla not met :                             0
sdwan preferred color not met :                 0
sdwan queue id :                                2
counter packets drop long:                      0
ulogging fw zp id:                              4
ulogging fw zone id array:                      3 3
ulogging fw class id:                           12544961
ulogging fw policy id:                          5559936
ulogging fw proto id:                           25
ulogging fw action:                             2
ulogging fw drop reason id:                     0
ulogging fw source ipv4 address translated:     0.0.0.0
ulogging fw destination ipv4 address translated:  0.0.0.0
ulogging fw source port translated:             0
ulogging fw destination port translated:        0
ulogging utd ips pri:                           1
```

```
ulogging utd ips sid:                              57756
ulogging utd ips gid:                              1
ulogging utd ips cid:                              21
ulogging utd urlf url hash:                        00000000000000000000000000000000
ulogging utd urlf url category:                    0
ulogging utd urlf url reputation:                  0
ulogging utd urlf application name:
ulogging utd amp dispos:                           0
ulogging utd amp filename hash:                    00000000000000000000000000000000
ulogging utd amp file type:                        0
ulogging utd amp file hash:                        0000000000000000000000000000000000000000000000000000000000000000
ulogging utd amp malname hash:                     00000000000000000000000000000000
ulogging utd drop reason id:                       0
ulogging sdvt drop reason id:                      0
ulogging utd ips policy id:                        1
ulogging utd ips action id:                        1
ulogging utd urlf policy id:                       N/A
ulogging utd urlf action id:                       N/A
ulogging utd amp policy id:                        N/A
ulogging utd amp action id:                        N/A
ulogging utd urlf reason id:                       0
ulogging ulogging flow direction:                  Reverse initiator
ulogging fw user name:
ulogging fw source ipv6 address translated:        ::
ulogging fw destination ipv6 address translated:   ::
ip dscp:                                           0x00
application name:                                  port dns
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.