Beveiligingsfuncties inschakelen met configuratiegroepen voor SDWAN

Inhoud

Inleiding

In dit document wordt beschreven hoe u NGFW, URL-filtering, AMP en IPS/IDS configureert via configuratiegroepen, inclusief instructies voor uniforme logboekregistratie.

Voorwaarden

Flow-zichtbaarheid en app-zichtbaarheid inschakelen

Als u beleidsgroepen gebruikt om beleid te definiëren:

- Selecteer Beleidsgroep en selecteer vervolgens Toepassingsprioriteit en SLA.
- Selecteer Nieuwe toevoegen
- Klik op Aanvullende instellingen en schakel de zichtbaarheid van de toepassing en de zichtbaarheid van de stroom in

Als u gebruik maakt van het legacy-beleid

- Selecteer een Cli-invoegprofiel in de configuratiegroep en voeg deze opdrachten toe

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

Zorg ervoor dat u voldoet aan de voorwaarden voor de functies zoals hier gegeven 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
```

Dit document richt zich op de functies die moeten worden ingeschakeld met behulp van beleidsgroepen

Next Gen Firewall (NGFW)

Om NGFW in te schakelen, voert u de stappen uit zoals vermeld:

- Selecteer Beleidsgroep en klik op NGFW en klik op NGFW-beleid toevoegen
- Geef het een beleidsnaam en klik op Volgende
- Selecteer de configuratiegroep die u wilt koppelen aan het NGFW-beleid
- Voeg de regels toe en klik op Volgende
- Maak uw NGFW-beleid

Om logboekregistratie in te schakelen, bewerkt u het NGFW-beleid en selecteert u Aanvullende instellingen en schakelt u Unified Logging in

URL-filtering

URL-filtering voor releases vóór 20.18 inschakelen:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Groepen van belang
- Selecteer Beveiliging en vouw vervolgens Profielen uit

Om URL-filtering voor releases 20.18 en later mogelijk te maken:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Objecten en profielen
- Beveiligingsprofielen selecteren

Selecteer URL-filtering toevoegen, voer de details in en klik op Opslaan

Advanced Malware Protection (AMP)

Om AMP in te schakelen voor releases vóór 20.18:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Groepen van belang
- Selecteer Beveiliging en vouw vervolgens Profielen uit

Om AMP in te schakelen voor releases 20.18 en later:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Objecten en profielen
- Beveiligingsprofielen selecteren

Selecteer Advanced Malware Protection en klik op Add Advanced Malware Protection

Voeg de gegevens toe en klik op Opslaan

Intrusion Prevention System (IPS)/Intrusion Prevention Detection (IDS)

IPS/IDS inschakelen voor releases vóór 20.18:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Groepen van belang
- Selecteer Beveiliging en vouw vervolgens Profielen uit

IPS/IDS inschakelen voor releases vanaf 20.18 uur:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Objecten en profielen
- Beveiligingsprofielen selecteren

Selecteer Inbraakpreventie en klik op Inbraakpreventie toevoegen

Voeg de gegevens toe en klik op Opslaan

Geavanceerd inspectieprofiel (AIP) maken

Om AIP in te schakelen voor releases vóór 20.18:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Groepen van belang
- Selecteer Beveiliging en vouw vervolgens Profielen uit

Om AIP in te schakelen voor releases 20.18 en later:

- Selecteer Configuratie op gebruikersinterface en vervolgens Beleidsgroep en klik vervolgens op Objecten en profielen
- Beveiligingsprofielen selecteren

Selecteer Geavanceerd inspectieprofiel en klik op Geavanceerd inspectieprofiel toevoegen

- Voer de AMP/IPS/URL-filternamen in die in de eerdere stappen zijn gemaakt en klik op Opslaan

Vereniging van AIP naar NGFW

- Selecteer Configuratie en selecteer vervolgens Beleidsgroepen en klik op NGFW
- Het eerder gemaakte NGFW-beleid bewerken
- Voor de eerder gemaakte NGFW-regels kunt u het eerder gemaakte AIP-profiel bewerken en koppelen en op Opslaan klikken

Ulogging

Voor het uitloggen schakelt u de functie op de router in via de configuratiegroep met behulp van

cli-invoegtoepassing

```
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
```

Verificatie

```
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
```

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.