Abilitare le funzionalità di sicurezza utilizzando i gruppi di configurazione per SDWAN

Sommario

Introduzione

In questo documento viene descritto come configurare NGFW, il filtro URL, AMP e IPS/IDS tramite i gruppi di configurazione, incluse le istruzioni per la registrazione unificata.

Prerequisiti

Consentire la visibilità del flusso e delle applicazioni

Se si utilizzano i gruppi di criteri per definire i criteri:

- Selezionare Gruppo di criteri, quindi selezionare Priorità applicazione e contratto di servizio.
- Selezionare Aggiungi nuovo
- Fare clic su Impostazioni aggiuntive e abilitare la visibilità dell'applicazione e del flusso

Se si utilizza il criterio legacy

- Selezionare un profilo aggiuntivo Cli nel gruppo di configurazione e aggiungere questi comandi

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

Accertarsi di soddisfare i prerequisiti per le funzionalità indicati di seguito 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
```

In questo documento vengono illustrate le funzionalità da abilitare tramite i gruppi di criteri

Next-Gen Firewall (NGFW)

Per abilitare NGFW, attenersi alla seguente procedura:

- Selezionare il gruppo di criteri, fare clic su NGFW, quindi su Aggiungi criterio NGFW
- Assegnare un nome al criterio e fare clic su Avanti
- Selezionare il gruppo di configurazione da associare al criterio NGFW
- Aggiungere le regole e scegliere Avanti
- Crea il tuo criterio NGFW

Per abilitare la registrazione, modificare il criterio NGFW, selezionare Impostazioni aggiuntive e attivare la registrazione unificata

Filtro URL

Per abilitare il filtro URL per le versioni precedenti alla 20.18:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Gruppi di interessi
- Selezionare Protezione, quindi espandere Profili

Per abilitare il filtro URL per le versioni 20.18 e successive:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Oggetti e profili
- Seleziona profili di sicurezza

Selezionare add url filtering, immettere i dettagli e fare clic su save (salva)

Advanced Malware Protection (AMP)

Per abilitare AMP per le versioni precedenti alla 20.18:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Gruppi di interessi
- Selezionare Protezione, quindi espandere Profili

Per abilitare AMP per le versioni 20.18 e successive:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Oggetti e profili
- Seleziona profili di sicurezza

Selezionare Advanced Malware Protection e fare clic su Add Advanced Malware Protection

Aggiungere i dettagli e fare clic su Salva

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

Per abilitare IPS/IDS per le versioni precedenti alla 20.18:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Gruppi di interessi
- Selezionare Protezione, quindi espandere Profili

Per abilitare IPS/IDS per le versioni 20.18 e successive:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Oggetti e profili

- Seleziona profili di sicurezza

Selezionare Prevenzione intrusioni e fare clic su Aggiungi prevenzione intrusioni

Aggiungere i dettagli e fare clic su Salva

Crea profilo di ispezione avanzata (AIP)

Per abilitare AIP per le versioni precedenti alla 20.18:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Gruppi di interessi
- Selezionare Protezione, quindi espandere Profili

Per abilitare AIP per le versioni 20.18 e successive:

- Selezionare Configurazione nell'interfaccia utente e quindi Gruppo di criteri e fare clic su Oggetti e profili
- Seleziona profili di sicurezza

Selezionare Profilo di ispezione avanzato e fare clic su Aggiungi profilo di ispezione avanzato.

- Immettere i nomi dei filtri AMP/IPS/Url creati nei passaggi precedenti e fare clic su Salva

Associazione di AIP a NGFW

- Selezionare Configuration, quindi selezionare Policy groups e fare clic su NGFW
- Modifica il criterio NGFW creato in precedenza
- Per le regole NGFW create in precedenza, modificare e associare il profilo AIP creato in precedenza e fare clic su Salva

Ulogging

Per il log, abilitare la funzionalità sul router tramite il gruppo di configurazione utilizzando il componente aggiuntivo 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
```

Verifica

```
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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).