Risoluzione dei problemi dei firewall basati su zone

Sommario

Introduzione

Questo documento contiene informazioni sulla risoluzione dei problemi per il firewall basato su zone.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Utilizzo della VPN con il firewall dei criteri basato su zone
- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Impossibile passare il traffico VPN

Problema

Il problema è che il traffico VPN non è in grado di passare attraverso il firewall basato su zone.

Soluzione

Consente al traffico del client VPN di essere ispezionato dal firewall Cisco IOS® basato su zone.

Ad esempio, ecco le righe da aggiungere alla configurazione del router:

```
access-list 103 permit ip 172.16.1.0 0.0.0.255 172.22.10.0 0.0.0.255

class-map type inspect match-all sdm-cls-VPNOutsideToInside-1
  match access-group 103

policy-map type inspect sdm-inspect-all
  class type inspect sdm-cls-VPNOutsideToInside-1
   inspect

zone-pair security sdm-zp-out-in source out-zone destination in-zone
  service-policy type inspect sdm-inspect-all
```

Impossibile passare GRE/PPTP

Problema

Il problema è che il traffico GRE/PPTP non è in grado di attraversare il firewall basato su zone.

Soluzione

Consente al traffico del client VPN di essere ispezionato dal firewall Cisco IOS basato su zone.

Ad esempio, ecco le righe da aggiungere alla configurazione del router:

<#root>

```
agw-7206>
enable

gw-7206#
conf t

gw-7206(config)#
policy-map type inspect outside-to-inside

gw-7206(config-pmap)#
no class type inspect outside-to-inside

gw-7206(config-pmap)#
no class class-default

gw-7206(config-pmap)#
class type inspect outside-to-inside

gw-7206(config-pmap-c)#
inspect

%No specific protocol configured in class outside-to-inside for inspection.
All protocols will be inspected
gw-7206(config-pmap-c)#
class class-default

gw-7206(config-pmap-c)#
drop

gw-7206(config-pmap-c)#
exit

gw-7206(config-pmap)#
exit
```

Controllare la configurazione:

<#root>

```
gw-7206#
show run policy-map outside-to-inside

policy-map type inspect outside-to-inside
 class type inspect PPTP-Pass-Through-Traffic
  pass
 class type inspect outside-to-inside
  inspect
 class class-default
  drop
```

Raggiungibilità della rete

Problema

Dopo aver applicato i criteri per il firewall basato su zone nel router Cisco IOS, le reti non sono raggiungibili.

Soluzione

Il problema potrebbe essere rappresentato dal routing asimmetrico. Il firewall Cisco IOS non funziona in ambienti con routing asimmetrico. Non si garantisce il ritorno dei pacchetti attraverso lo stesso router.

Il firewall Cisco IOS tiene traccia dello stato delle sessioni TCP/UDP. Per una manutenzione accurata delle informazioni sullo stato, un pacchetto deve partire e tornare dallo stesso router.

Impossibile passare il traffico DHCP attraverso un firewall basato su zona

Problema

Impossibile passare il traffico DHCP attraverso un firewall basato su zona.

Soluzione

Per risolvere il problema, disabilitare l'ispezione del traffico di zona.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- AnyConnect su IOS con ZBFW (Zone-Based Firewall)

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).