Knowledge Base

SIP-Konfiguration auf der Fortigate

Datum	05/01/2011 09:21:00
Hersteller	Fortinet
Modell Type(n)	Fortigate
Firmware	v4.2
Copyright	Boll Engineering AG, Wettingen
Autor	Sy
Dokument-Version	1.0

Situation:

SIP-Traffic auf einer Firewall zuzulassen ist nicht ganz einfach, wenn man nicht den einen Portrange von mehreren 10‘000 Ports öffnen möchte.

Die Fortigate bietet für den SIP Traffic spezielle Unterstützung: den SIP Session Helper und das SIP Application Layer Gateway.

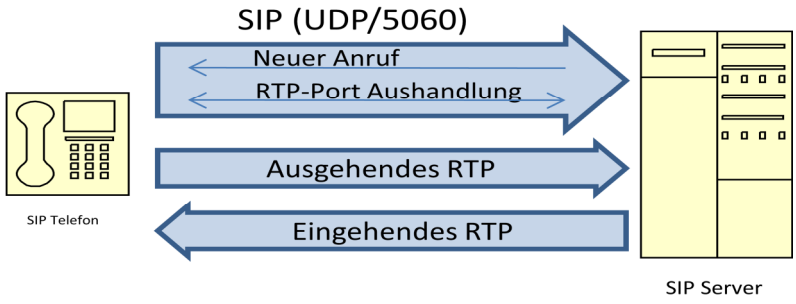
Wie diese zu konfigurieren sind und was diese bewirken, wird in dem folgenden Artikel beschrieben.

Lösung:

Das SIP Protokoll

SIP benutzt zur Signalisierung typischerweise UDP (manchmal auch TCP) auf Port 5060 (für TLS-verschlüsseltes SIP meist Port 5061). Typischerweise baut der SIP-Client diese Verbindung zum SIP-Server auf.

Die Sprachübertragung erfolgt jedoch über RTP-Verbindungen. Um die eigene Sprache zu senden wird eine ausgehende RTP-Verbindung erstellt, um die Sprache des Gegenübers zu hören, hat man eine eingehende Verbindung (aus Sicht des Sprechenden).



Für RTP sind keine festen Ports festgelegt. Je nach Implementation wird ein anderer Portrange angegeben. Typischerweise bewegt sich der Portrange in UDP/8000-35000.

Welcher Port für eine jeweilige RTP-Verbindung verwendet wird, wird in der SIP-Verbindung auf Port 5060 abgemacht.

Je nach Implementation ist es ebenfalls möglich, dass die RTP-Verbindung direkt zum anderen Gesprächspartner führt und nicht zum SIP-Server.

Für die richtige Konfiguration der Firewall ist es nun wichtig zu wissen, von wo nach wo der SIP-Verkehr und von wo nach wo der RTP-Verkehr (aus Sicht der Firewall) läuft.

Steht z.B. die Firewall zwischen SIP Telefon (private IP) und SIP Server (public IP) ergeben sich typischerweise folgende Probleme:

- Theoretisch müsste sowohl für die ausgehende als auch für die eingehende RTP-Verbindung der Portrange UDP/8000-35000 geöffnet werden (für den eingehenden Traffic wäre dann noch ein NATting der Ziel-Adresse notwendig, da das Telefon eine private IP hat und diese vom Internet her nicht angesprochen werden kann. Security-technisch nicht sehr sinnvoll.
- Die Firewall NATted zwar die ausgehende SIP-Verbindung, aber leider wird innerhalb der SIP-Verbindung auch die private IP des SIP-Telefons übergeben, welche vom SIP-Server angesprochen wird.

Eine Firewall, die das SIP-Protokoll unterstützt, muss diese Probleme behandeln.

- SIP-NAT: wenn die Firewall im Header der SIP-Pakete NATted, so muss sie ebenfalls in der Verbindung nach IP-Adressen suchen und diese NATten
- RTP-Pinholing: damit auf der Firewall nicht mehrere 10.000 Ports ein- und ausgehend geöffnet werden müssen, muss die Firewall den SIP-Traffic mitverfolgen und die dort ausgehandelten RTP-Ports on demand öffnen und nach dem Telefonat sofort wieder schliessen. Auch hier muss das NATting der Firewall selber mitberücksichtigt werden.
-

Die Fortigate bietet zwei verschiedene Varianten, um das SIP-Protokoll zu unterstützen: der SIP Session Helper und das SIP Application Layer Gateway (ALG)

Der SIP Session Helper

Der SIP Session Helper ist eine einfache und schnelle Möglichkeit, das SIP-Protokoll in einfachen Netzwerkkonfigurationen zu unterstützen. Sowohl das SIP-NATting als auch das RTP Pinholing wird von dem Session Helper durchgeführt.

Der Session Helper arbeitet per default auf Port UDP/5060 und kann nur im CLI konfiguriert werden:

```
config system session-helper
…
    edit <id>
        set name sip
        set port 5060
        set protocol 17
    next
…
end
```

Knowledge Base

SIP-Konfiguration auf der Fortigate

Diese Einstellung ist eine globale Konfiguration (pro VDOM) und muss nicht in den entsprechenden Firewall Regeln explizit aktiviert werden. Sobald die Fortigate Traffic auf Port UDP/5060 erkennt, schaltet sich der Session Helper automatisch ein.

Um den Session Helper zu löschen, muss der entsprechende Eintrag im CLI gelöscht werden:

```
config system session-helper
    delete <id>
end
```

Um den SIP Session Helper auf einen anderen Port zu aktivieren, muss dieser hier geändert werden

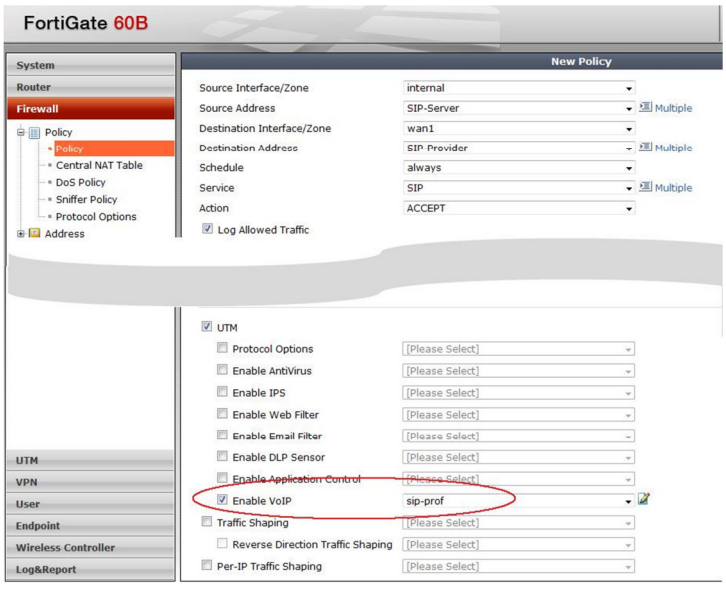
```
config system session-helper
    edit <id>
        set port <neuer Port>
    next
end
```

(Obwohl das Löschen und die Portänderung sofort nach Eingabe der jeweiligen CLI Befehle wirksam werden sollten, wurde bereits festgestellt, dass manchmal noch ein Reboot der Fortigate notwendig ist. Im Zweifelsfall muss also ein Reboot in Erwägung gezogen werden).

Das SIP Application Layer Gateway (ALG)

Der SIP ALG bietet die gleichen Funktionen wie der SIP Session Helper. Zusätzlich liefert der ALG Funktionen, um das Netzwerk vor SIP Attacken zu schützen, die Anzahl von SIP Sessions zu limitieren, eigene Einstellungen zum Idle Werten vorzunehmen, Syntax der SIP Befehle zu prüfen und detailliertes Logging der SIP-Verbindungen aufzuzeichnen.

Im Gegensatz zum SIP Session Helper muss der SIP ALG in den Firewall Policies aktiviert werden. Dieses geschieht durch das Aktivieren eines VoIP Profiles.



Knowledge Base

SIP-Konfiguration auf der Fortigate

Der SIP ALG lauscht typischerweise auf Port UDP 5060. Falls dieser geändert werden muss, kann das im CLI erfolgen:

```
config system settings
    set sip-tcp-port <neuer udp port>
    set sip-udp-port <neuer tcp port>
end
```

Obwohl im FortiOS-Handbuch für SIP festgestellt wird, dass der der SIP ALG den SIP Session Helper übersteuert, wird vom Support empfohlen, den SIP Helper zu löschen, sobald der SIP ALG eingeschaltet wird.

SIP Troubleshooting

SIP Session Helper:

`diagnose sys sip debug-mask <debug_mask_int>`	Zum Setzten des Debug Levels. Verschiedene Debug Masks bewirken verschiedene Debug Levels
`diagnose sys sip dialog list`	Zum Auflisten aller SIP-Verbindungen, die vom Session Helper kontrolliert werden
`diagnose sys sip dialog clear`	Zum Löschen aller SIP-Verbindungen, die vom Session Helper kontrolliert werden
`diagnose sys sip mapping list`	Zum Auflisten aller SIP-NATs
`diagnose sys sip status`	Für eine Uebersicht, was der Session Helper gerade macht

SIP ALG:

`get test sip <test_level_int>` `diagnose test application sip <test_level_int>`	Anzeige von SIP ALG Informationen
`diagnose sys sip-proxy calls list`	Auflisten aller SIP-Calls, die vom ALG verarbeitet werden
`diagnose sys sip-proxy calls clear`	Löschen aller SIP-Calls, die vom ALG verarbeitet werden
`diagnose sys sip-proxy filter <filter_options>` `diagnose sys sip-proxy log-filter <filter_options>`	Filterungsmöglichkeit für die obigen beiden Befehle
`diagnose sys sip-proxy meters list`	Anzeige von aktiven SIP rate limits
`diagnose sys sip-proxy stats list`	Auflisten von Status Informationen der aktiven SIP calls
`diagnose sys sip-proxy stats list`	Löschen dieser Statistiken

Sonstiges

Weitere Einstellungen und Informationen können Sie dem Fortinet Handbuch „VoIP-Solutions: SIP“ (http://docs.fortinet.com/fgt/handbook/fortigate-voip-sip-40-mr2.pdf) entnehmen.