Alcadis
confidence in connectivity

TECHNOTE

Ruckus ICX configuratie – SSH

Versie: 1.1
Auteur: Herwin de Rijke / Willem Fieggen
Datum: 28 juni 2018

Inhoud

1 Inleiding

In dit document wordt beschreven op welke manier u SSH configureert voor een Ruckus ICX switch.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met de manier waarop bij een Ruckus ICX switch SSH wordt ingesteld.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel die een Ruckus ICX switch willen configureren en hier nog weinig ervaring mee hebben.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- Basiskennis van IPv4
- Basiskennis van VLAN's
- Basiskennis Ruckus FastIron Command Line Interface

1.4 Verdere documentatie

Er zijn nog veel meer configuratie opties en wellicht dat deze configuratie niet precies aansluit bij de door u gewenste toepassing. Hiervoor verwijzen wij graag naar de diverse manuals voor deze productlijn van de fabrikant zoals de Ruckus FastIron Security Configuration Guide of de Ruckus FastIron Command Reference Guide.

1.5 Ondersteunde platformen

De informatie in deze Technote is toepasbaar op alle modellen in de Ruckus ICX serie.

De instructies die in dit document gegeven worden zijn op basis van firmware versie Version 08.0.70a. Wij raden aan om uw switch te upgraden naar deze versie of hoger. Mogelijk zijn in andere versies als gebruikte versies bepaalde functies niet beschikbaar of is de werking anders.

2 SSH instellen

Standaard is de switch op IP niveau alleen via telnet bereikbaar. Data die via telnet verstuurd wordt is niet versleuteld. Dit houdt in dat derden het management verkeer tussen administrator en switch kunnen inzien wat in het algemeen als ongewenst wordt gezien. Daarom is het raadzaam alleen via beveiligde protocollen in te loggen op de switch en de standaard, onbeveiligde protocollen, uit te zetten.
SSH maakt gebruik van certificaten waarmee het management verkeer versleuteld wordt. Standaard is de switch niet via SSH toegankelijk en dient dit apart geconfigureerd te worden.

2.1 SSH configuratie bekijken

```
device(config)#show ip ssh config
SSH server                  : Disabled
SSH port                    : tcp\22
Host Key                    :
Encryption                  : aes256-cbc, aes192-cbc, aes128-cbc, aes256-ctr, aes192-ctr,
aes128-ctr, 3des-cbc
Permit empty password       : No
Authentication methods      : Password, Public-key, Interactive
Authentication retries      : 3
Login timeout (seconds)     : 120
Idle timeout (minutes)      : 0
SCP                         : Enabled
SSH IPv4 clients            : All
SSH IPv6 clients            : All
SSH IPv4 access-group       :
SSH IPv6 access-group       :
SSH Client Keys             : RSA(0)
device(config)#
```

2.2 SSH configuratie aanpassen

Om SSHv2 toegang te kunnen verlenen aan het Ruckus apparaat dient met onderstaande commando een Crypto Key aangemaakt te worden. Omdat de software standaard een DSA sleutel aanmaakt, gebruiken we de RSA parameter om in plaats van een DSA sleutel een RSA sleutel aan te maken.

```
device(config)# crypto key generate rsa
```

2.3 SSH idle timeout instellen

Standaard blijven SSH sessies onbeperkt open staan. Om dit gedrag te veranderen dient de standaard idle timeout in minuten ingesteld te worden met het commando:

```
device(config)#ip ssh idle-time 30
```

2.4 Resultaat

```
device(config)#show ip ssh config
SSH server                  : Enabled
SSH port                    : tcp\22
Host Key                    : RSA 1024
Encryption                  : aes256-cbc, aes192-cbc, aes128-cbc, aes256-ctr, aes192-ctr,
aes128-ctr, 3des-cbc
Permit empty password       : No
Authentication methods      : Password, Public-key, Interactive
Authentication retries      : 3
Login timeout (seconds)     : 120
Idle timeout (minutes)      : 30
SCP                         : Enabled
SSH IPv4 clients            : All
SSH IPv6 clients            : All
SSH IPv4 access-group       :
SSH IPv6 access-group       :
SSH Client Keys             : RSA(0)
```

2.5 Telnet toegang uitzetten

Nu er beveiligde toegang mogelijk is is het raadzaam onbeveiligde toegang te ontzeggen. Om de switch ontoegankelijk te maken voor toegang via het Telnet protocol gebruikt u het volgende commando:

```
device(config)#no telnet server
```