Enabling SSH

It always starts with the generation of a public/private keypair that will be only used for the SSH-process. In this command we use a dedicated label "SSH-KEY" which we later assign to the SSH-config. The default-keylength is typically too small, it's time to move to a stronger crypto. For new setups I only use 4096 Bit keys, however, 2048 is still widely used. Thats more than recommended on sites like http://www.keylength.com and makes the session-setup a little slower. But by far not that slow that it's unusable. And it typically doesn't hurt to have better crypto then the others.

Getting Started:

You will need to ensure that you have a domain name configured, for example: home.lab or example.com. Let's get started

Generate Domain name

```
switch(config)#ip domain-name home.lab
```

Generate RSA-Keypair at 4096bits

```
switch(config)# crypto key generate rsa label SSH-KEY modulus 4096
```

The RSA-Keypair is assigned to the SSH-config:

```
switch(config)#ip ssh rsa keypair-name SSH-KEY
```

Allow only SSH Version 2

```
switch(config)#ip ssh version 2
```

Set Minimum Diffie-Hellman Key exchange

```
switch(config)#ip ssh dh min size 4096
```

When the SSH-session is established, the session-keys are computed with the Diffie-Hellmann key exchange protocol. By default this is done with 768 Bit, which is not state-of-the-art any more. For my setups (with MacOS and Linux clients) I configure a bitlength of 4096 Bit. You should use a powerful terminal like SecureCRT or use only a size of 2048 Bit which is still very secure. And if your IOS is too old, this command will also not be available.

SSH Logging

```
switch(config)#ip ssh logging events
```

The last step is to restrict the vty-lines to only use SSH, so that Telnet is not allowed any more:

```
switch(config)#line vty 0 4
 switch(config-line)#transport input ssh
```

If the IOS-device is running at least 15.5(2), then it's possible to disable unwanted algorithms. In security-audits, all CBC-ciphers are often a problem.

Revision #2
Created 5 January 2022 12:57:53 by Brian
Updated 26 April 2022 21:13:59 by Brian