AUTHENTICATION ALGORITHMS

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The Junos OS uses the following authentication algorithms:

- Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

  To verify that the message has not been tampered with, the Junos OS compares the calculated message digest against a message digest that is decrypted with a shared key. The Junos OS uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with authentication header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

- Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. The Junos OS uses the SHA-1 HMAC variant that provides an additional level of hashing. SHA-1 can be used with AH, ESP, and IKE.

- SHA-256, SHA-384, and SHA-512 (sometimes grouped under the name SHA-2) are variants of SHA-1 and use longer message digests. The Junos OS supports the SHA-256 version of SHA-2, which can process all versions of Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption.

Power Point Shortcut Key

Action	Power point shortcut
Bold	Ctrl-B
Close	Ctrl-W
Close	Ctrl-F4
Copy	Ctrl-C
Find	Ctrl-F
Italics	Ctrl-I
Menubar	F10
New slide	Ctrl-N
Next window	Ctrl-F6
Open	Ctrl-O
Paste	Ctrl-V
Print	Ctrl-P
Repeat Find	Shift-F4
Repeat/Redo	Ctrl-Y
Replace	Ctrl-H
Save	Ctrl-S
Slide Show: Begin	F5
Slide Show : Black screen show/hide	B
Slide Show: End	Esc
Slide Show : Erase annotations	E
Slide Show: Go to next hidden slide	H
Slide Show : Hide pointer and button always	Ctrl-L
Slide Show: Hide pointer and button temporarily	Ctrl-H
Slide Show: Mouse Pointer to arrow	Ctrl-A
Slide Show : Mouse pointer to pen	Ctrl-P
Slide Show : Next slide	N
Slide Show: Previous slide	P
Slide Show: Set new timings while rehearsing	T
Slide Show : Stop/ restart automatic slide show	S
Slide Show: Use mouse-click to advance (rehearsing)	M O
Slide Show : Use original timings	W
Slide Show: White screen show / hide	F7
Spelling and Grammer Check	Ctrl-F6
Switch to the next presentation window	Ctrl-Tab/Ctrl-Page Down
Switch to the next tab in a dialog box	Ctrl-Shift-F6
Switch to the previous presentation window	Ctrl-Shift-Tab / Ctrl-page Up
Switch to the previous tab in a dialog box	Num/
Turn character formatting on or of	Ctrl-U

Underline Undo	Ctrl-Z