Quantcom

TCP AO

Next generation of BGP session authentication

Zbyněk Pospíchal, Quantcom a.s.

European Peering Forum, September 2024, Vienna

AO = Authentication Options
RFC 5925

Key Benefits

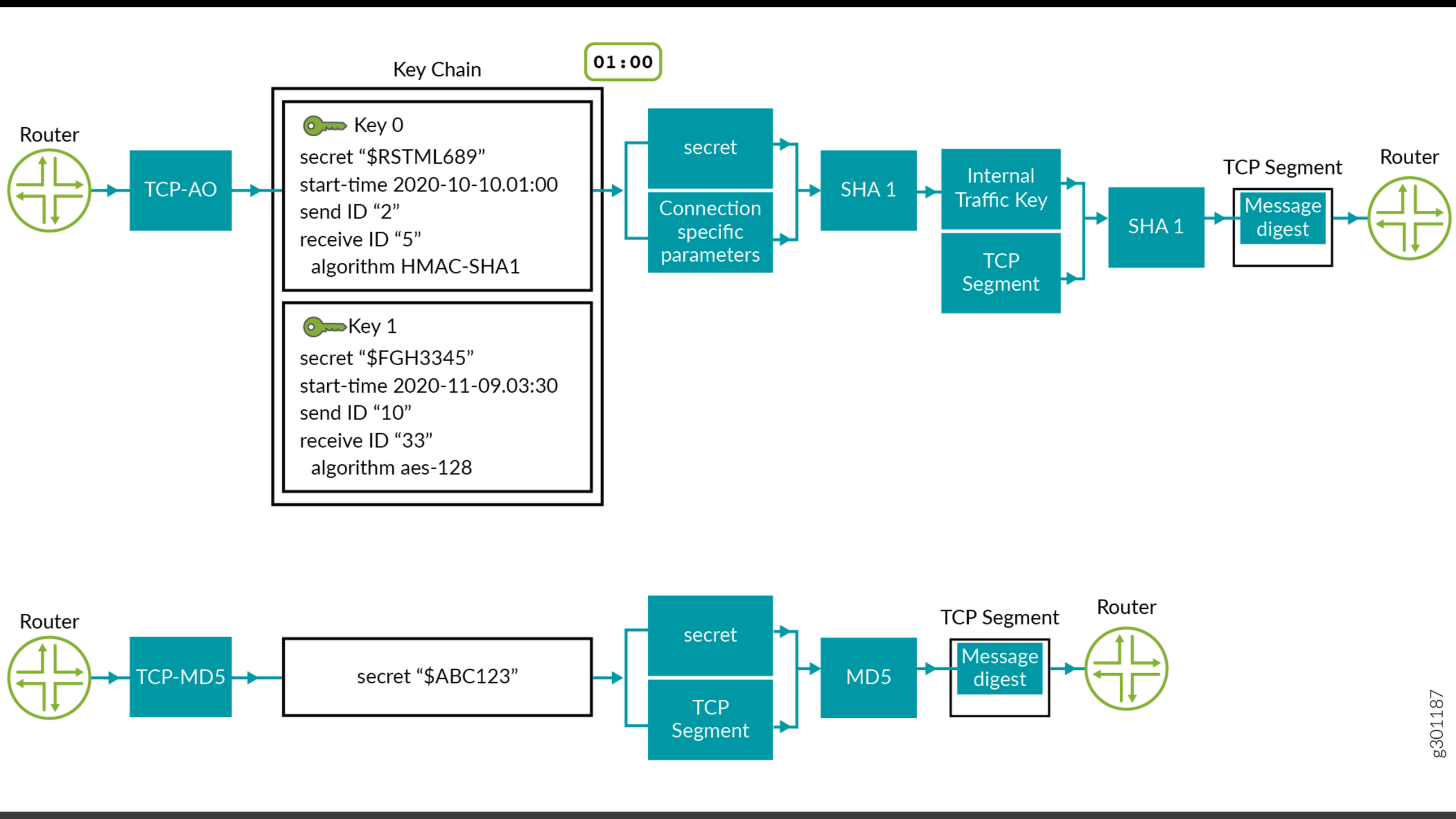
Key Benefits

Improved security
(~~MD5~~, SHA-1, AES-128)

Key Benefits

Improved security
(~~MD5~~, SHA-1, AES-128)

Better key management


Router
TCP-AO
Key Chain
01:00
Key 0
secret "$RSTML689"
start-time 2020-10-10.01:00
send ID "2"
receive ID "5"
algorithm HMAC-SHA1
Key 1
secret "$FGH3345"
start-time 2020-11-09.03:30
send ID "10"
receive ID "33"
algorithm aes-128
secret
Connection specific parameters
SHA 1
Internal Traffic Key
TCP Segment
SHA 1
TCP Segment
Message digest
Router
Router
TCP-MD5
secret "$ABC123"
secret
TCP Segment
MD5
TCP Segment
Message digest
Router
g301187

IOS XR

```
tcp ao
 keychain FENIX-AO
  key 1 SendID 100 ReceiveID 100
 !
!

key chain FENIX-AO
 key 1
  accept-lifetime 00:00:00 september 18 2023 infinite
  key-string password 613523DFA7233327MZ151495C45414B
  send-lifetime 00:00:00 september 18 2023 infinite
  cryptographic-algorithm AES-128-CMAC-96
 !
!
```

JunOS

```
key-chain KEYSET3 {
    key 1 {
        secret "$9$C8gXaBRSyeMLxdb4JDmQUuO1Rcef99NVaP5n9puIS"; ##
SECRET-DATA
        start-time "2024-1-1.00:00:00 +0100";
        algorithm ao;
        ao-attribute {
            send-id 100;
            recv-id 100;
            tcp-ao-option enabled;
            cryptographic-algorithm aes-128-cmac-96;
        }
    }
}
```

IOS XR

```
router bgp 23456
 neighbor-group NIX-BV4X
  bfd fast-detect
  bfd multiplier 5
  bfd minimum-interval 200
  ao FENIX-AO include-tcp-options enable
  ttl-security
  graceful-restart
  address-family ipv4 unicast
   maximum-prefix 2000 95 restart 15
   next-hop-self
   send-community-ebgp
   route-policy NIX-BV4-IN in
   route-policy NIX-BV4-OUT out
   remove-private-AS
   soft-reconfiguration inbound
  !
 !
!
```

JunOS

```
protocol bgp family inet group NIX4 {
  neighbor 100.100.100.100 {
      description FENIX-TEST-PEER;
      ttl 255;
      family inet {
         unicast {
            prefix-limit {
               maximum 2000;
               teardown {
                  95;
                  idle-timeout 15;
               }
            }
         }
      }
      authentication-algorithm ao;
      authentication-key-chain KEYSET3;
      peer-as 23456;
      bfd-liveness-detection {
         minimum-interval 200;
         multiplier 5;
      }
   }
```

Real world experience

Started in November 2023

7 peering partners with TCP-AO enabled
(over DE-CIX, NIX.CZ, SIX.SK, VIX.AT)
some also with ENHE/RFC8950

Stable support in IOS XR and JunOS

Peering automation tools usually
consider RFC2385 MD5 auth support
as an end of the history...

So is TCP-AO worth it?

--> BGP over QUIC (!!!)

IETF draft-retana-idr-bgp-quic-05

Questions?