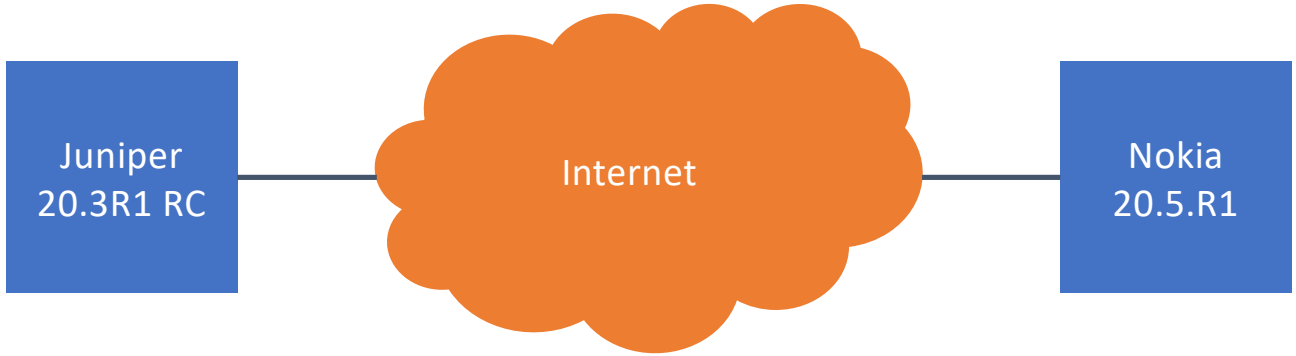
TCP-AO Interop and Some Exciting News

IETF 112 TCPM – November 11, 2021

Melchior Aelmans, Juniper Networks
Greg Hankins, Nokia

Juniper and Nokia Interop Test Results



- Successful interop test using TCP-AO for BGP finished in June 2020
- Established multihop IPv4 and IPv6 BGP sessions over the Internet
- No need to meet or bring routers for testing in person
- Tested with HMAC-SHA-1-96 and AES-128-CMAC-96 algorithms

Lessons Learned #1 – Send and Receive Are Configured From the Router's Perspective

Juniper

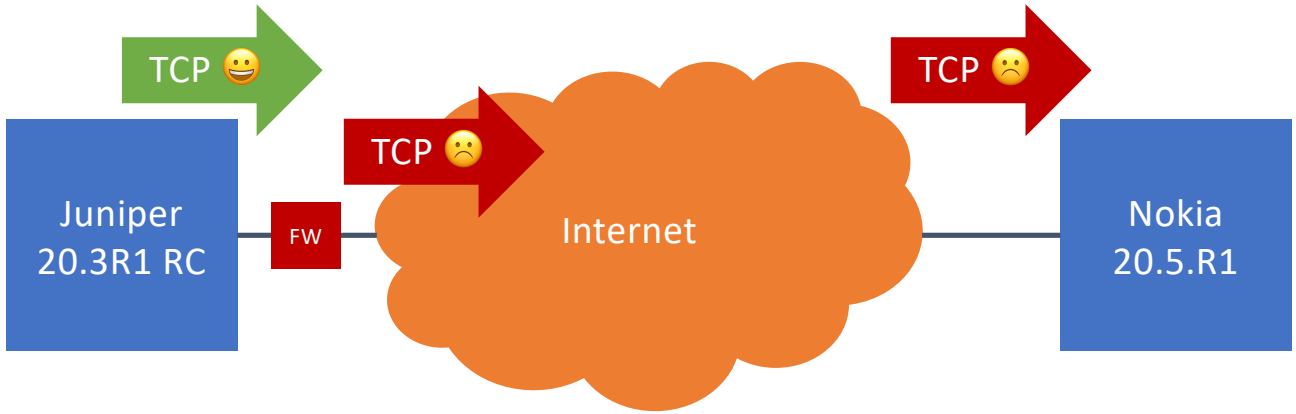
```
# show security authentication-key-chains
key-chain ao_aes_chain {
    key 0 {
        secret
"$9$xk3NVYq.53/taZnCu1yrwYg4UHf5F/A0z3"; ## SECRET-
DATA
        start-time "2020-6-16.01:00:00 +0530";
        algorithm ao;
        ao-attribute {
            send-id 9;
            recv-id 2;
            tcp-ao-option enabled;
            cryptographic-algorithm aes-128-cmac-96;
        }
    }
}
```

Nokia

```
configure system security {
    keychain "interoptest-aes" {
        tcp-option-number {
            receive tcp-ao
            send tcp-ao
        }
        receive {
            entry 9 {
                authentication-key
"yzClLKIFsAVR91AobUXUT/ppPzL7bVxBrNNg" hash
                algorithm aes-128-cmac-96
                begin-time 2020-06-09T04:00:00.0Z
            }
        }
        send {
            entry 2 {
                authentication-key
"yzClLKIFsAVR91AobUXUT/ppPzL7bVxBrNNg" hash
                algorithm aes-128-cmac-96
                begin-time 2020-06-09T04:00:00.0Z
            }
        }
    }
```

- Send and receive IDs must match each other
- TCP-AO supports multiple algorithms, make sure you are using are the same one
- Feedback provided for TCP YANG model

Lessons Learned #2 – Firewalls May Change TCP Headers



- The TCP MSS option was modified by a firewall in the path between the routers
- This caused the MAC calculation to fail on the receiver and the BGP session would not come up

✓The TCP-AO option worked as expected to protect against modified packets 😀!

Implementation Status

- Commercial implementations
  - Cisco: IOS XR 6.6.3 and 7.0.1
  - Huawei: targeted for Q2 2021 – does anyone know?
  - Juniper: 20.3R1 (20.3R1 release candidate tested with Nokia)
  - Nokia: 16.0.R15, 19.10.R7 and 20.5.R1 (interop tested with Juniper)
- Open source implementations
  - None, this is a problem...
- Tools
  - Wireshark
  - Missing other tools support (tcpdump, etc.)

Exciting news!

- An open source development project funded by the RIPE NCC has just started
- Implemented by Philip Paeps (FreeBSD committer since 2003)
  - Implementation support and router VMs provided by Juniper and Nokia
- Deliverables
  - Reference implementation of TCP-AO for FreeBSD and nc(1)
  - Port of the FreeBSD reference implementation to the Linux kernel
  - If we find more sponsors: extensions to the OpenBGPD and BIRD routing daemons
- Release targeted for January 2022

Resources

- Interoperable configuration examples for Cisco, Juniper, Nokia
  https://github.com/TCP-AO/Configuration-examples
- Under development now: TCP-AO technology evangelism, resources, and central location for everything
  https://www.tcp-ao.net
  - Content is kept in GitHub, contributors welcome!

Questions?

Melchior Aelmans - maelmans@juniper.net

Greg Hankins - greg.hankins@nokia.com