eduVPN 2.0

TNC19 – Forging Digital Societies

Release Schedule

- **eduVPN 1.0**: July 2017
- **eduVPN 2.0**: April 2019
- **eduVPN 3.0**: Q4 2019?

End of Life of release *n* == release date of eduVPN *n+2*

Release Process

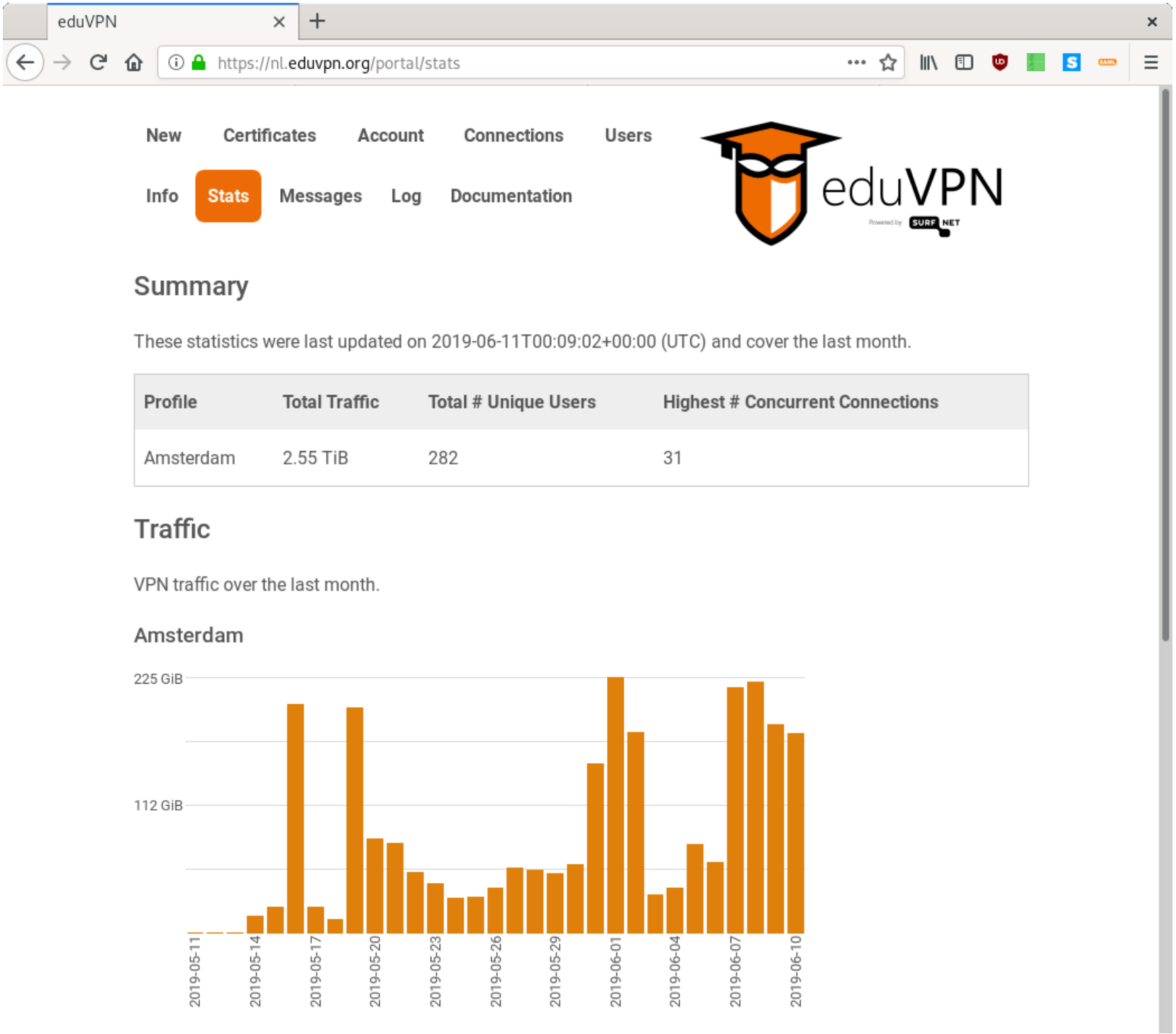
- **eduVPN 1.0**: “rolling release” with feature updates, bug fixes, security fixes and configuration (template) updates
- **eduVPN 2.0**: only bug fixes / security updates

What’s New?

Portal

Merge “Admin” and “Portal”

- Avoid (code) duplication
  - Share authentication
  - Share UI


eduVPN
https://nl.eduvpn.org/portal/stats
New
Certificates
Account
Connections
Users
Info
Stats
Messages
Log
Documentation
eduVPN
Powered by SURF NET
Summary
These statistics were last updated on 2019-06-11T00:09:02+00:00 (UTC) and cover the last month.
Profile
Total Traffic
Total # Unique Users
Highest # Concurrent Connections
Amsterdam
2.55 TiB
282
31
Traffic
VPN traffic over the last month.
Amsterdam
225 GiB
112 GiB
2019-05-11
2019-05-14
2019-05-17
2019-05-20
2019-05-23
2019-05-26
2019-05-29
2019-06-01
2019-06-04
2019-06-07
2019-06-10

VPN Security

Tighten VPN Configuration

- Always use “tls-crypt”
- Fully remove *compression (framing)* support (VORACLE)

Permissions

Rework Permissions

- Permissions are used to
  - Decide who gets access to which VPN profile(s)
  - Decide who’s an *admin*

#road2tnc

Permissions

User Permissions in eduVPN 1.0

- “Real time” validation of permissions
  - SAML: attributes/claims
  - LDAP: attributes
  - VOOT (REST query)
  - Static Configuration

Permissions

User Permissions in eduVPN 2.0

- “During authentication” retrieval of permissions
  - SAML: attributes/claims
  - LDAP: attributes

Dropped support for VOOT / Static Configuration...

Permissions

Why?

- SAML has no way to retrieve attributes “out of band” when using the Web SSO profile
- Requires hook “on connect” to validate permissions
  - Weak point during connection setup
  - Delay when connecting

Permissions

Problem: How do we make sure we have (reasonably) up to date permissions for a particular user?

Permissions

- How?
  - Periodically *force* users, by expiring the “session” to reauthenticate, thus obtaining a fresh list of permissions...
    - Server default: after 90 days
  - Bind OAuth token and issued X.509 certificate(s) to this session expiry

Two Factor Authentication

Two Factor Authentication (2FA):

- Remove asking for 2FA credentials during connection establishment...
- Move 2FA to “authentication” phase
  - Allows for using 3rd party services for 2FA
  - Removes “on connect” hook, simplifies and makes VPN connections more robust
  - Removes “annoyance”, e.g. after suspend

Two Factor Authentication

Deprecation for “embedded” 2FA?

- 2FA is in the interest of the *organization* deploying the VPN server, *not* the user!
  - Move 2FA to “IdP”!
- Remove all 2FA support from eduVPN itself for 3.0?

New Template System

- Use very simple multi language aware template system
  - Simple “human readable” translation files
  - High speed native template engine

OAuth Tokens

- Improved Public key cryptography for VPN *Guest* Usage scenario
  - From *libsodium* tokens to standardized JWT with EdDSA tokens (Ed25519)
  - Support Key IDs (kid)
    - No longer need to iterate over all (known) public keys when excepting “foreign” tokens

#road2tnc

Software Quality

- Reduce number of (external) dependencies
  - Less is more (usually)
- Remove weak points in the design
  - Do not put querying external services in the *critical path*
- Reduce lines of code
  - The best code is code not written...
- Increased use of *static code analysis* tools during development...

Lessons Learned

- These are of course all obvious and I really should have known better...
  - Somehow, somewhere, someone uses features of the old version that got removed in the new version...
    - “addEntityId” of Mellon (SAML)
    - Static Groups authentication
  - Replacing A with B results in cascade of (unrelated) failures all over the place...

Questions / Remarks?

- Follow us on Twitter: **@eduvpn_org**
- The Web: https://www.eduvpn.org/
  - **With regularly updated blog!**
- Mail: eduvpn-support@lists.geant.org