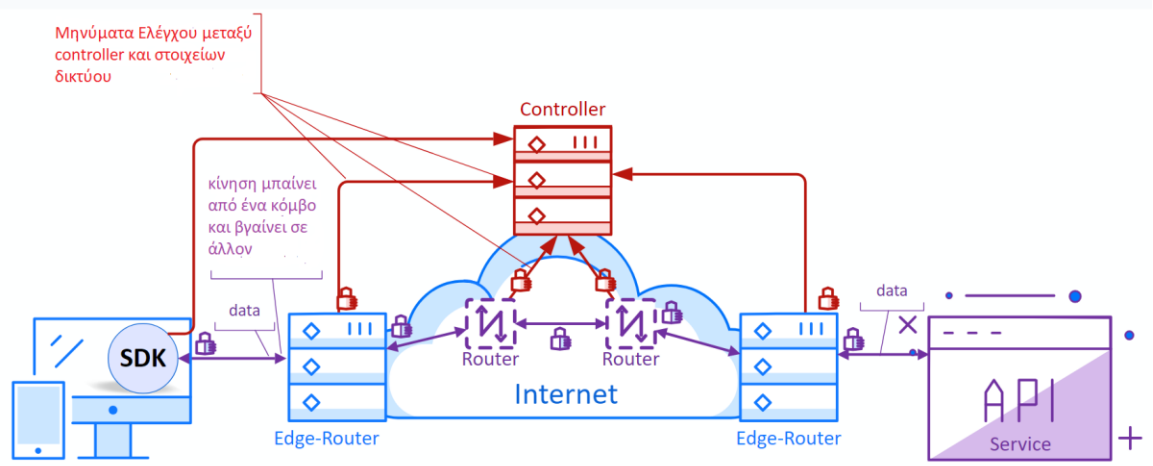
Zero Trust Networking με το Open Ziti

Περιγραφή

Η αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust) δημιουργήθηκε με σκοπό οι περιοχές δικτύων να σταματήσουν να υποθέτουν προϋπάρχουσα εμπιστοσύνη λόγω προϋπάρχουσας γνώσης σε οποιαδήποτε οντότητα εντός ή εκτός των εγκαταστάσεών της. Η προϋπάρχουσα γνώση μπορεί να εκφράζεται π.χ. ως το όνομα χρήστη, η τοποθεσία/όνομα ενός υποδικτύου και τις εφαρμογές κοκ. Η νέα αρχιτεκτονική απαιτεί από όλους τους συντελεστές ασφαλούς λειτουργίας (συσκευές, χρήστες και εφαρμογές) να αποδεικνύουν ένα επίπεδο ασφαλούς λειτουργίας/πιστοποίησης διαφορετικά δεν αποκτούν πρόσβαση στο δίκτυο.

Πολλές εταιρείες (π.χ. Cisco, Microsoft, Fortigate) παρέχουν λύσεις Zero trust Networking. Στην παρούσα διπλωματική θα χρησιμοποιηθεί η ανοικτή αρχιτεκτονική OpenZiti (https://openziti.io/docs/learn/introduction/). Στην αρχιτεκτονική OpenZiti υπάρχουν: α) ένα overlay δίκτυο mesh που υλοποιείται από tunnels, β) ακραίοι δρομολογητές για την επιβίβαση/αποβίβαση της κίνησης γ) ένας ελεγκτής(controller), και δ) SDK που επιτρέπουν τον έλεγχο και εφαρμογή εμπιστοσύνης στην τελική εφαρμογή.



Η αρχιτεκτονική openziti έχει υλοποιήσει/τροποποιήσει υφιστάμενες εφαρμογές web server[1], browZer κλπ. Στην υπάρχουσα διπλωματική καλείστε α) να στήσετε μια τοπολογία openziti[2,3] β) να τροποποιήσετε την εφαρμογή curl ή wget π.χ μέσω tlsuv[4] ώστε να είναι μπορεί να συνδέεται σε ένα περιβάλλον openziti γ) και δ) την εφαρμογή ανοικτού κώδικα Context broker[5] και να κάνετε μετρήσεις π.χ HTTP GET/POST που να δείχνουν εάν η αρχιτεκτονική επηρεάζει τις επιδόσεις των εφαρμογών.

Επικοινωνία: Ε. Συκάς (sykas@cn.ntua.gr) , Δ. Καλογεράς (dkalo@noc.ntua.gr , τηλ. 210-7721863)

[1] https://github.com/openziti/ngx_ziti_module
[2] https://openziti.discourse.group/t/how-to-start-an-openziti-simple-instance-with-docker-compose/1483
[3] https://openziti.io/docs/learn/quickstarts/services/ztha/
[4] https://github.com/openziti/tlsuv
[5] https://github.com/telefonicaid/fiware-orion