Technical Disclosure Commons

Defensive Publications Series

November 20, 2018

# IDENTITY AND CLEANUP OF AUTHORIZATION SESSION WORK IN A SOFTWARE-DEFINED ACCESS ENABLED INTERNET OF THINGS NETWORK

Sanjay Hooda

Syam Appala

Eliot Lear

# IDENTITY AND CLEANUP OF AUTHORIZATION SESSION WORK IN A SOFTWARE-DEFINED ACCESS ENABLED INTERNET OF THINGS NETWORK

AUTHORS:
Sanjay Hooda
Syam Appala
Eliot Lear

## ABSTRACT

Techniques are described herein for making identity work when inline tagging is not supported. This may apply to an Internet of Things (IoT) network connected to a Software Defined Access (SDA) edge.

## DETAILED DESCRIPTION

Software Defined Access (SDA) for Internet of Things (IoT) is transforming IoT networks. However, there are some issues with IoT switches. Many switches do not propagate Security Group Tag (SGT) tags and have limited Ternary Content-Addressable Memory (TCAM) space. Moreover, IoT deployments are in Layer-2 rings, and switch Application-Specific Integrated Circuits (ASICs) cannot do Virtual Extensible Local Area Network (VXLAN) encapsulation.

Accordingly, it is desired to ensure that when SDA is extended to IoT, both identity and policy are provided across the whole spectrum. Techniques described herein enable extending identity, segmentation, and policy with an SDA connected IoT switches without compromising security.

Consider a SDA network with an IoT enabled ring of switches with identity and policy download from a security engine.

First, clients are joined to the security engine. This is the initial stage when the client joins the extended node (EX-3 in this example). Figure 1 below illustrates the identity process from the endpoint to the security engine using EX-3.

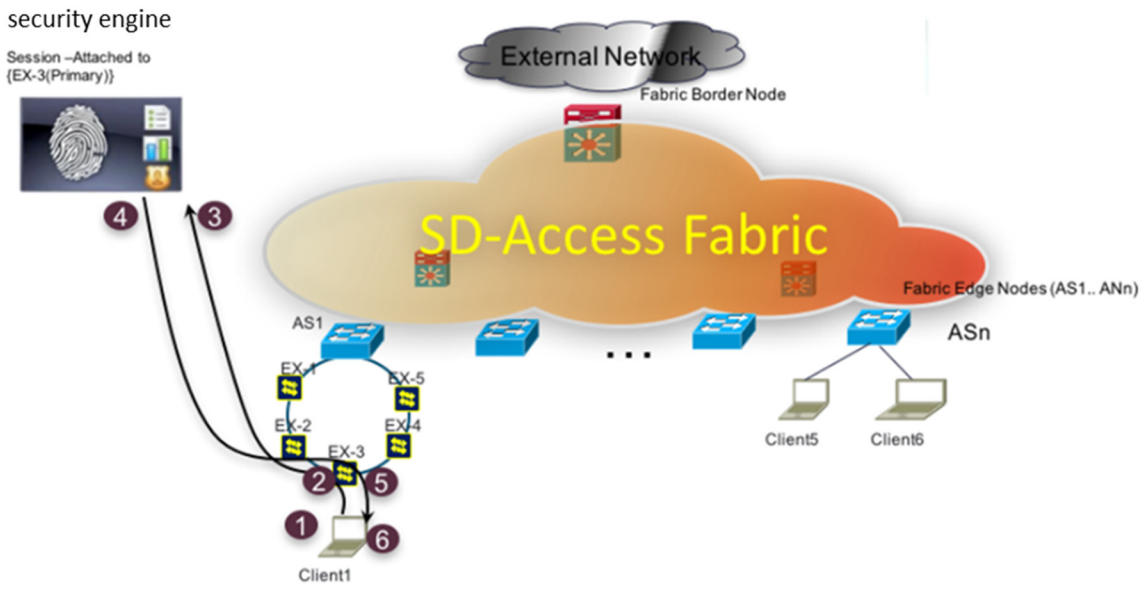


*Figure 1*

During the identity process of the client the following steps take place. At 1, the client connects to the network. At 2, Switch EX-3 is configured with the (dot1x) and starts the authentication process with the security engine. At 3, the security engine receives the authentication request. At 4, the security engine authenticates and creates a session that the user/device authenticates on switch EX-3. EX-3 in this case is marked as “primary.” At 5, switch EX-3 now allows the client traffic.

Now that identity at the directly connected switch is established, authorization is propagated in the rest of the network to the fabric edge AS1. Figure 2 below illustrates identity (authorize only) from EX-2, EX-1, and Fabric Edge (AS1).

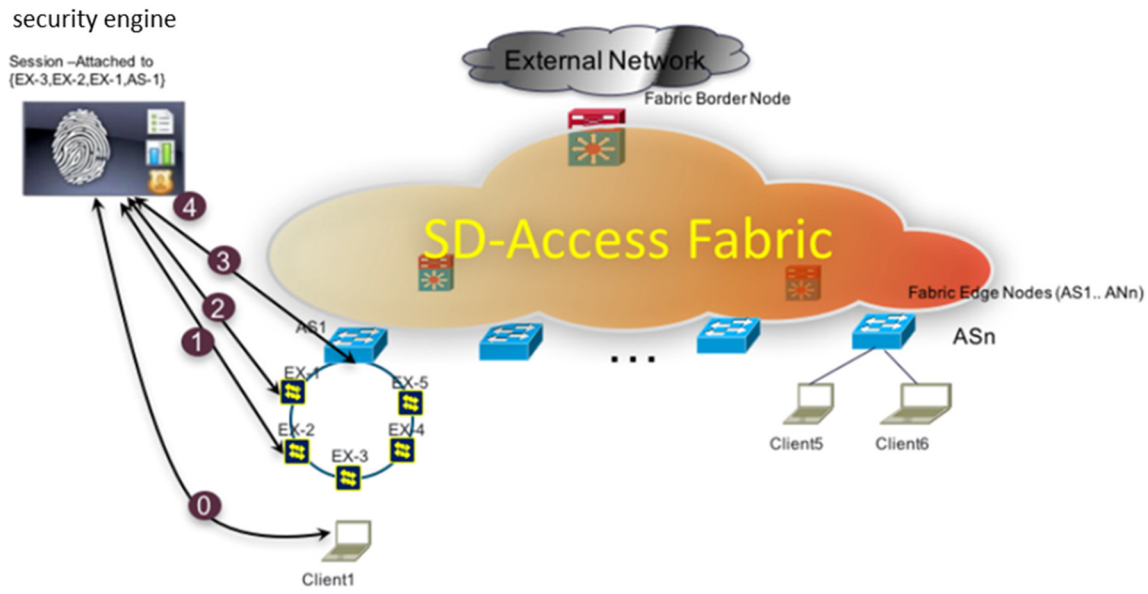


*Figure 2*

During authorization for the next level of switches the following steps take place. At 0, the initial authentication from Figure 1 occurs. This is depicted in Figure 2 above for completeness. At 1, 2, and 3, switches in the path to the fabric edge are configured to send authorize only requests which are used to download the "group tag" from the security engine. At 4, the security engine receives the authorize only requests from EX2, EX1, and AS1. The security engine may add these as secondary devices having the session for client-1. This additional information in the session for EX2, EX1, and AS1 may be used during cleanup of the session.

To clean up the state, Figure 3 below illustrates the primary and secondary session information to be used for cleanup. In particular, shown is cleanup of a state on EX-2, EX-1, and AS1 when the endpoint is removed.

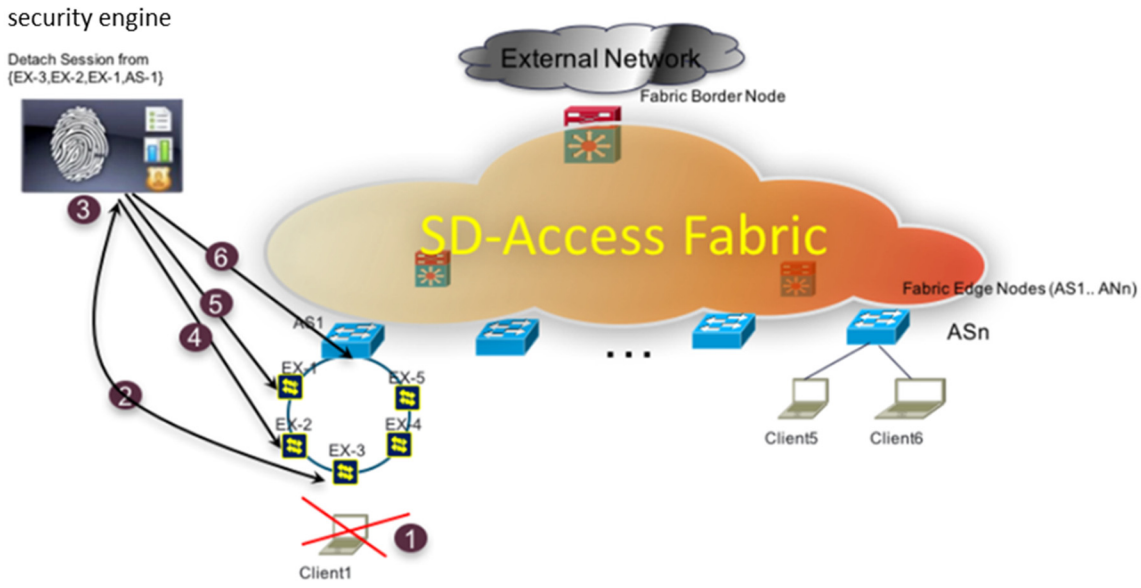


*Figure 3*

At 1, the client is removed. At 2, EX-2 cleans up the client state and informs the security engine about the removal of the client. At 3, the security engine looks up in its session table and finds that there are other secondary switches where the authorization session was attached (i.e., EX-2, EX-1, and AS1). At 4, 5, and 6, the security engine sends the message to clean up the state on the devices for the clients.

Thus, making the above changes to the identity works in IoT scenarios. The addition of an authorization only flow, combined with a separate authentication flow on a directly connected (EX-1) device along with authorization flows on the neighboring and edge switches, enables a consistent policy to be delivered to both fabric and non-fabric devices.

In summary, techniques are described herein for making identity work when inline tagging is not supported. This may apply to an IoT network connected to a SDA edge.