RSAConference2018

Singapore | 25–27 July | Marina Bay Sands

#RSAC

SESSION ID: SDS-R03

BLOCKCHAIN FOR CYBERSECURITY – MICRO-SEGMENTED NETWORK ACCESS CONTROL

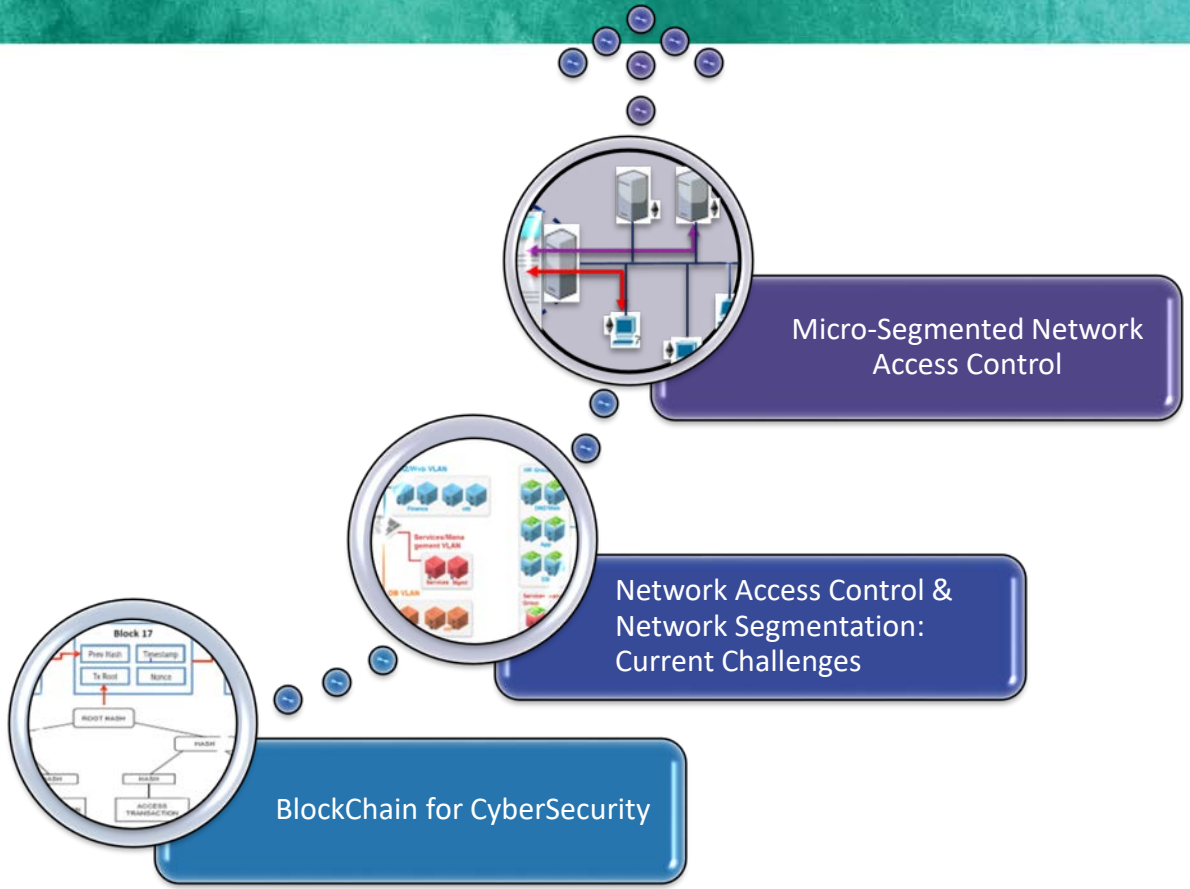
Rajeevan Kallumpuram CISSP, CISM

Assistant Vice President
Reliance Industries Limited
Twitter- @RajeevansView

BLOCKCHAIN -

One of the most disruptive technologies in the recent times…!!!

Agenda

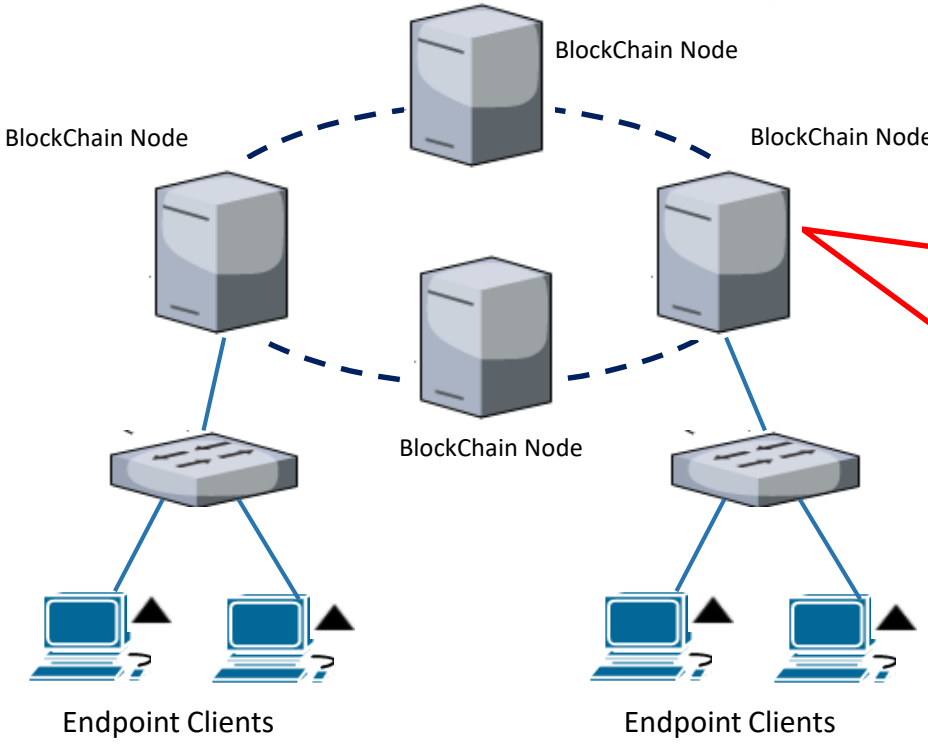

Micro-Segmented Network Access Control
Network Access Control & Network Segmentation: Current Challenges
BlockChain for CyberSecurity

BLOCKCHAIN FOR CYBERSECURITY

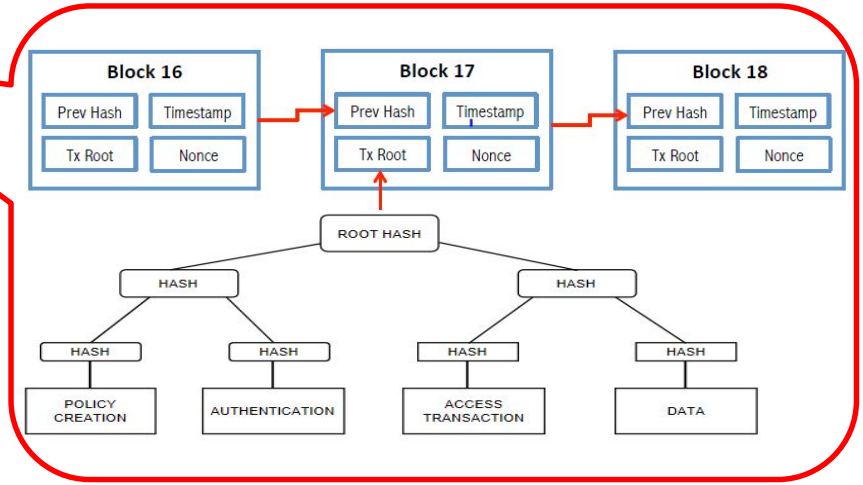
BlockChain as a Technology - Key Features

BlockChain - Scope in CyberSecurity

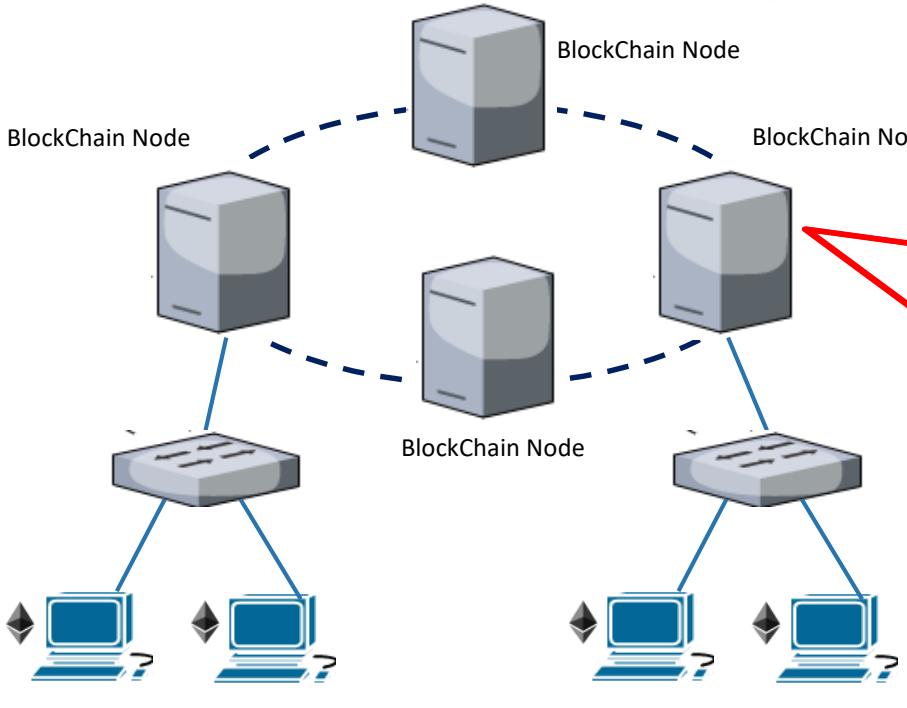
BlockChain: Basic Architecture



Blocks of Records

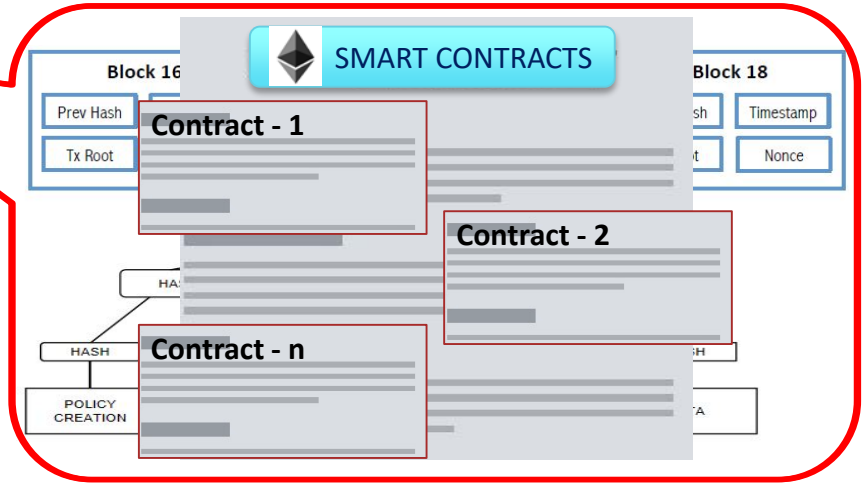


Smart Contracts on BlockChain



Agent/Wallet

Blocks of Records



BlockChain - Key Features

- Identity Management
- Decentralized Org Structure
- Distributed Consensus
- Redundancy by Design
- Immutability

Use-case Scenario – Securing Servers and Endpoints

- Common Methods for Securing Endpoint Devices –
  - Network Access Control (NAC) solutions
  - Minimum Baseline Security Standards
  - Endpoint Security Solutions
  - Patching & Vulnerability Management

- Common Methods for Securing Servers –
  - Network Segmentation and access control policies
  - Server Hardening/Lockdown
  - Vulnerability & Threat Management
  - Network & Host based Security Solutions

NAC & NETWORK SEGMENTATION: HOW THEY HELP…?

What Are NAC & Network Segmentation?

Implementation Challenges

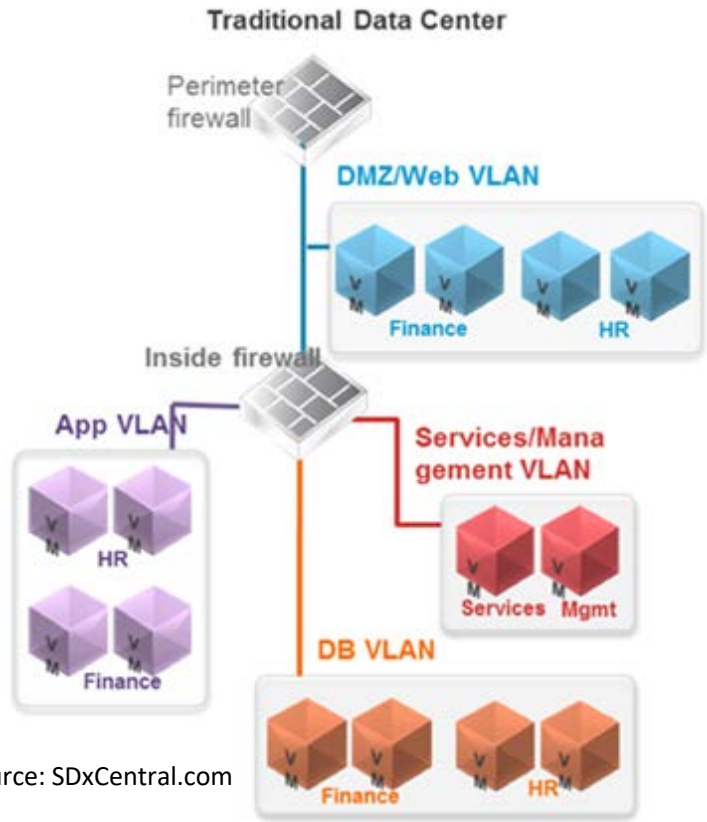
Network Access Control (NAC)

- Control access to the Corporate network based on a predefined set of device health and host integrity parameters of Endpoint Devices.
- Once the network access made available, further access control on specific servers/systems on the network needs to be handled by other network or system security solutions.

Traditional NAC – Challenges and Pain Areas

- NAC is a combination of user authentication, endpoint security assessment and access control. There are many working pieces (e.g., AD, LDAP, Token Services, MDM etc.) that must be integrated. Achieving the required level of interoperability is a real challenge.
- Challenges in Device Profiling and Security Posture checking due to the diversity of device types and operating systems.
- Vague network boundaries.
- NAC hasn't been an outright failure, but for many enterprises, NAC has not met the expectations or the needs.

Network Segmentation and Access Control



Source: SDxCentral.com

- Network segmentation is the practice of splitting a network into subnetworks, each being a network segment, primarily aiming at boosting performance and improving security.
- It splits the network into zones that contain data with similar compliance requirements.
- Access between segments are controlled using ACL's on Firewalls or other network devices.
- Segmentation helps to limit the attack surface available to pivot-in if one of the hosts on the network segment is compromised.

Micro-Segmentation: Feature Enhancements

- A method of creating secure zones in a network that allows isolation and granular control of communication between hosts.
- Micro-segmentation allows security policies to be defined by workload, applications, VM, OS etc., for greater attack resistance.
- Traditional perimeter security systems inspect the traffic coming into the network in a north-south direction. Whereas Micro-segmentation limits east-west traffic between systems, making it difficult for a hacker to explore the network laterally.

Source: SDxCentral.com

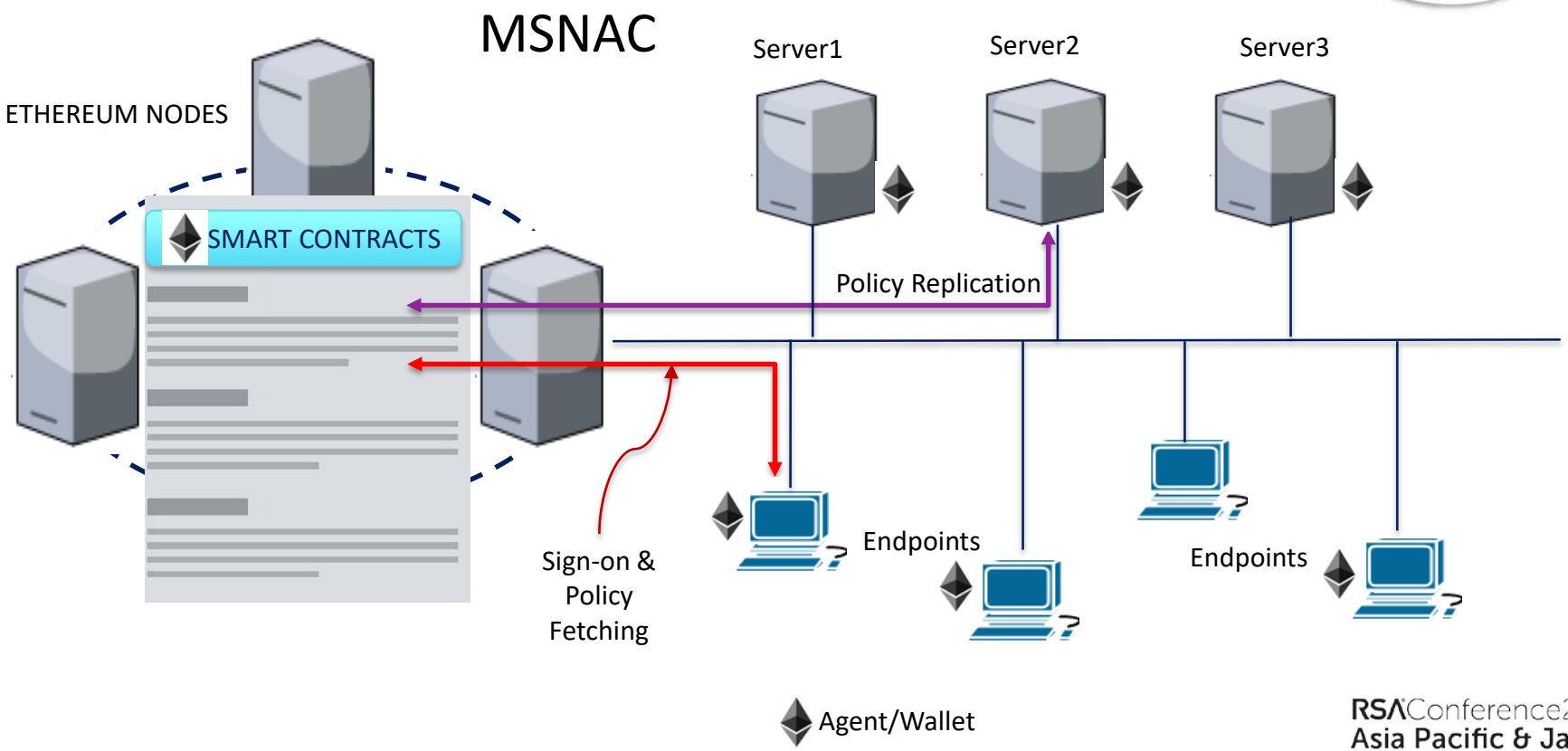
Micro-Segmentation – Scope for Improvements

- Real-time automated enforcement of access control policies
- Identify the presence of “Trusted Endpoints” and dynamically allow optimum level of access on servers/applications.
- External/Untrusted devices to have bare minimum access, defaulting to the access levels on public facing web applications.

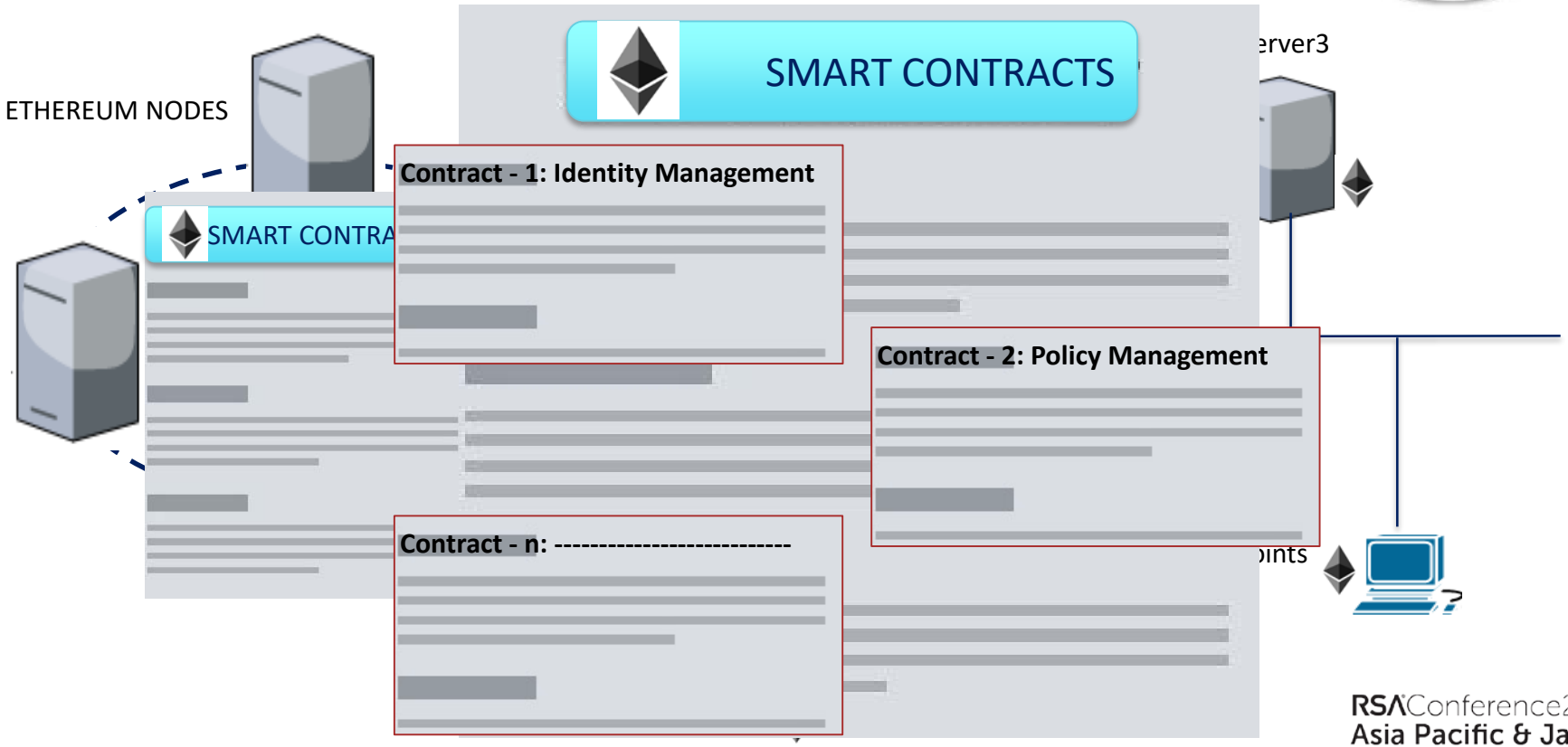
MICRO-SEGMENTED NETWORK ACCESS CONTROL

Solution Proposition : BlockChain based Micro-Segmented NAC

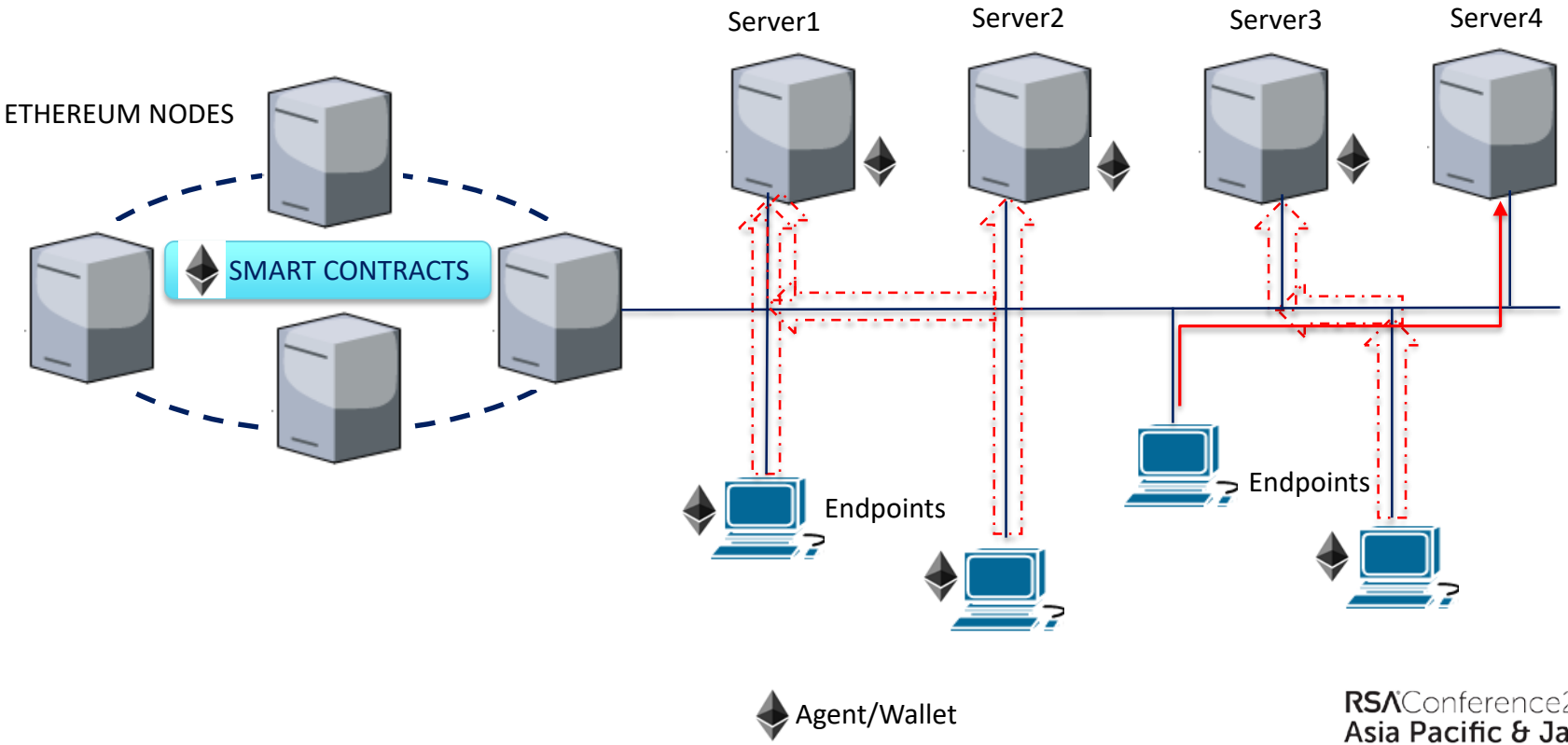
Micro-Segmented NAC Architecture



Smart Contracts - Building Blocks of MSNAC



Micro-Segmented NAC : Prototype



Micro-Segmented NAC : Process Flow

Device Policies

User signs onto his/her device.

- The Device Agent submits the authentication request to the respective Smart Contracts on the BlockChain

BlockChain Smart Contract authenticates the user

- Responds back to the Device Agent with the Access Policy corresponding to this specific Device-User combination

Device Agent enforces the Policy on the local client device.

Server Policies

Policies on the Server Agents sync up near-realtime with the BlockChain

Policies are enforced to allow access only on required/ published ports and NOT on any other ports available on the server.

Device -> Server Access

Servers verify all the service requests against the locally enforced policies. These local policies get synced near-realtime with BlockChain.

The requests will be served or denied according to the Policy verification.

- Policy verification results get stored in the BlockChain Ledger

MSNAC is Better – Why & How…?

- Benefits of MSNAC over other point solutions
  - Unified Solution combining the key functionalities of Identity & Access Management, Micro-segmentation, NAC and BlockChain.
  - Easier orchestration between modules and easier management.
  - Strong and secure Identity Management based on public key cryptographic algorithms.
  - 3-Level Authentication & Authorization, based on the combination of User, Device and Server/Application.
  - Near-Realtime policy update and enforcement.
  - Access Control Policies get enforced at the source and destination endpoints, thus reducing unwanted white-noise traffic on the network.
  - Easier and most authentic access tracking – The transactions are captured and preserved on an immutable BlockChain ledger.

Summary

- Technology Basics and key features of BlockChain
- Challenges in implementing NAC & Network Segmentation
- Solution proposition – Micro-Segmented NAC, combining major features of NAC and Micro-segmentation and also leveraging the key features and functionalities of BlockChain technology

Way Forward…

- Refresh your knowledge and understanding of BlockChain technology and the available Blockchain platforms.
- Consider designing & implementing a Micro-Segmented NAC solution, customized for your network environment.
- Identify the need and potential use-cases, especially CyberSecurity use cases, of BlockChain in your respective Business environments.

QUESTIONS…?

THANK YOU

Rajeevan Kallumpuram

Assistant Vice President
Reliance Industries Limited

Rajeevankk@gmail.com
Twitter- @RajeevansView