Arista Networks Multi-Domain Macro-Segmentation Service Group (MSS-G)

Group-based Network Segmentation for Enterprise Mobility, IoT and Cloud

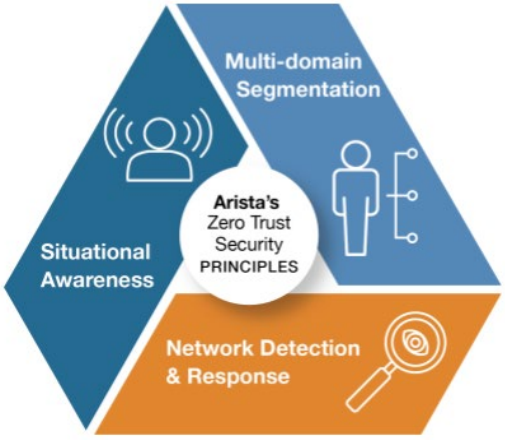
Enterprises are going through digital transformation driven by trends such as migration to the cloud, mobile workforce and explosion of different IT, OT & IoT devices connecting to the network for delivering many new services.

This accelerated pace of change coupled with a vanishing network perimeter and ever-changing threat landscape is posing many security challenges and leading to a rise in various cyberattacks e.g. Ransomware and Malware, vulnerability exploits or many insider threats attacking IoT/endpoints connected to the network. These growing threats need to be identified & contained quickly otherwise could result in huge losses of revenue and customers as well as risk the company's reputation.

Zero trust is a framework for securing enterprises in today's modern digital transformation.

Zero trust assumes there is no network perimeter & based on the "Never Trust Always Verify" approach, that requires organizations to continuously monitor and validate all users, devices, applications & transactions independent of their location and validate them against the appropriate privileges and several attributes to protect against new threats or any suspicious or out of compliance activities.

Arista's Zero trust Network architecture is aligned with NIST 800-207[1] and represented by 3 pillars as depicted in the diagram below.



Zero Trust Framework

- Situational Awareness → Visibility of all assets & workloads
- Enforcement → Restrict access to required connections
- Continuous Monitoring → Never trust continually verify

Zero Trust Assumes

- Successful authentication is not sufficient
- Device and User visibility beyond simple fingerprinting
- Client agents are not possible with many IoT devices

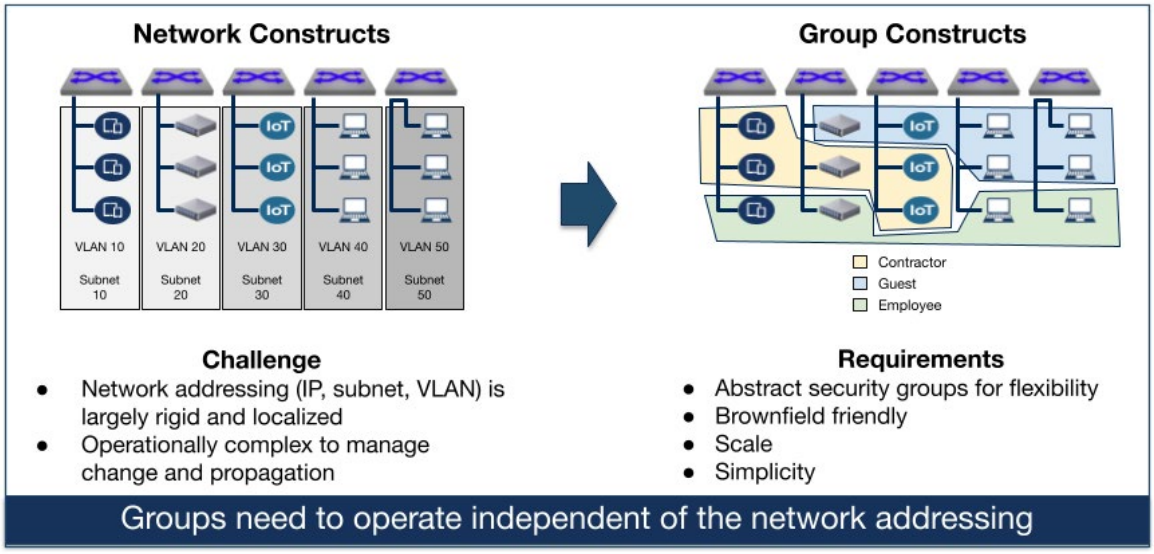
[1] *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf*

Arista Zero Trust Networking Architecture is built on the same cloud principles which have become best practices across Datacenter, Campus and Cloud networks that uses Highly available leaf-spine network from Arista, Network Automation using Arista CloudVision, Telemetry for real-time visibility, monitoring and troubleshooting and Programmability & open APIs at every layer to allow faster integration with Arista ecosystem partners or any 3rd party system of choice.

This paper covers Arista's Group-based Multi Domain Segmentation, one of the pillars of Arista Zero Trust Architecture in more detail.

While Network Segmentation is an effective way for reducing attack surface and limiting damage caused in one part of the network from proliferating to the entire network, traditional approaches based on network constructs (IP, subnet, VLANs..etc) or Access Control Lists (ACLs) are too rigid & operationally complex to manage, implementing those methods requires not only re-architecting the network but also managing thousands of ACLs manually on device-by-device basis.

Enterprises require a segmentation approach that is flexible i.e. independent of the network constructs (IP, subnets, VLANs..Etc.), can scale and be simple to deploy considering both brownfield & greenfield environments.



What is MSS-Group

MSS-Group or Group-Based Network Segmentation, part of Arista's Zero Trust Networking Architecture, allows classification of endpoints into segments and security policy definition between those segments to allow or deny access. A given segment contains a set of endpoints that should have identical security properties within the network. Policies are then defined between segments rather than between endpoints and enforced on Arista EOS devices in hardware.

MSS-Group Key Benefits

- Flexible: Separates group policy from Network address boundaries
- Simplified: No complex overlay protocols to configure & manage
- Scalable: Efficient use of Data Plane Resources to overcome ACL Scale challenges
- Standards-based Ethernet implementation: No-proprietary tags, can co-exist with 3rd party switches in network as long as enforcement is done on Arista Switches
- Dynamic policy integration with ecosystem partners (e.g. Forescout)

Use-cases

Enterprise with Users, IT & OT

Campuses and branches connecting different types of users (Employees, IT admin, Security-staff...etc), IT devices (Printers, Video Conferencing systems, IT Infrastructure e.g Switches/Routers, Servers...etc) and OT devices (Security Cameras, Badge Readers, Building automation system, HVAC..etc) placed in different segments, irrespective of their location but depending on their security need and controlling access using segment policies

Examples:

1. Allow access from Segment-1 (Employees) to Segment-11 (Printers, Video Conferencing)
2. Allow access from Segment-2 (Security-staff) to Segment-12 (Security Camera, Badge Readers)
3. Allow access from Segment-3 (IT admin) to Segment-13 (IT Infrastructure)
4. Deny access for everything else not matching above policies (Default-Policy)

Compliance & Regulation

PCI DSS (Payment Card Industry Data Security Standard) and HIPAA (Health Insurance Portability and Accountability Act) require protecting cardholder data and patient health records respectively. Network segmentation using MSS-G can help reduce the scope of compliance assessment by consolidating card holder data or patient health records into selective segments, controlling access thru MSS-G segment policies & thus minimizing the risk.

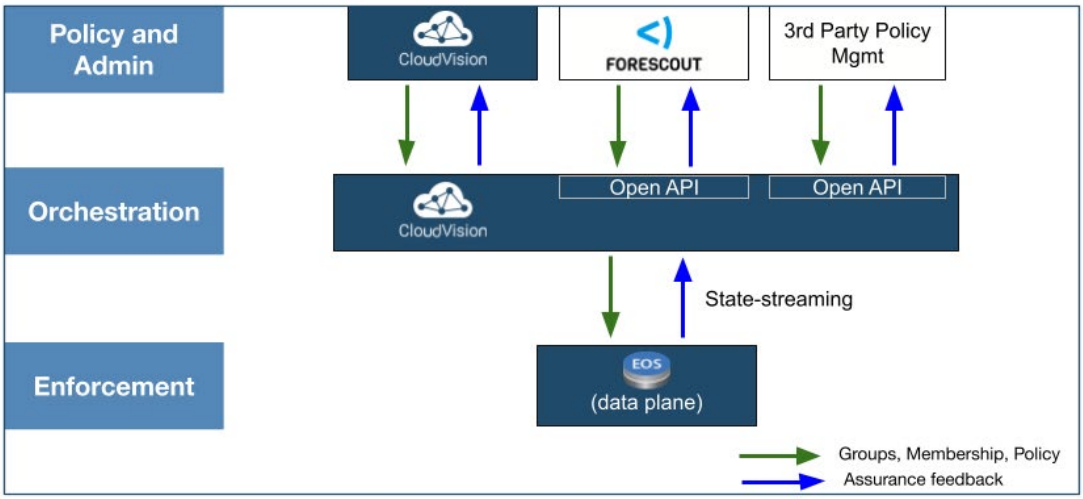
Manufacturing Facility & Distribution Center

Segmenting resources for facilities, plants, production lines & corporate network in different groups and controlling access through MSS-G segment policies.

Deployment Options

Customers have flexibility to use different options for deployment as below:

- Arista CloudVision contains a built-in studio that allows users to define segments, assign devices to segments, create segment policies and apply the policy enforcement across the Network. CloudVision dashboard also provides an easy way to visualize and monitor any inter-segment forwarded and dropped traffic.
- For dynamic policy, Forescout EyeSight and EyeSegment integrated with Arista CloudVision's open APIs deliver a complete Zero Trust Solution by continuous discovery & monitoring of endpoints connected to switches, dynamically assign these endpoints to Groups, define segmentation policies and enforce these policy across the network through Arista CloudVision.
- Customers who would prefer their own policy management solution can connect to CloudVision through open APIs or even manage switches directly using Arista EOS CLI or EAPI.



Conclusion

MSS-G or Group-Based Network Segmentation, part of Arista's Zero Trust Networking Architecture is a simple, non-proprietary, flexible & scalable security solution for segmenting users, IT, OT and IoT devices. MSS-G can effectively reduce attack surface, limit the scope of compliance & regulation assessment & thus overall reduce the risk for organizations.

Reference:

https://www.arista.com/assets/data/pdf/Whitepapers/Arista-Zero-Trust-Security-for-Cloud-Networking.pdf

https://www.arista.com/assets/data/pdf/Whitepapers/Network-Automation-CloudVision-Studios-WP.pdf

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062