Zero Trust Networking for Government

Zero trust security for mission-critical networks

Solution sheet

Alcatel·Lucent Enterprise

In today's high-tech world, zero trust network security has become a critical concern for governments. In fact, cybersecurity has become so critical, that the **zero trust network security** architecture has become the "Gold Standard" for LAN networking. Whether it's stealing subscriber, employee, customer, or taxpayer data, or holding entire company networks for ransom, the critical nature of network security has exploded before us and with it the recognition that networks once thought secure — are probably no longer.

For government departments and agencies, using the most secure equipment available, has become not only critical, but is now a matter of survival. For agencies to continue to operate and to support the missions they are assigned, cyber-attacks must be addressed head-on.

Fortunately, Alcatel-Lucent Enterprise has stepped to the forefront with the Alcatel-Lucent OmniSwitch® family of products, delivering the capabilities required to ensure government networks have the security required to meet today's challenges.

We enable Government departments and agencies to:

- Support mission-critical systems:
  - ¬ Alcatel-Lucent OmniSwitch-based networks are secure, autonomous, self-adaptive, flexible and so durable they have a lifetime warranty
  - ¬ intelligent Fabric (iFab) technology automates the deployment of the network, network elements and devices
  - ¬ IoT containment automatically classifies and onboards IoT devices and places them into secure containers (virtual networks) based on their permitted roles
- Deploy highly secure and zero trust networks
- Provide resilient connectivity in harsh environments
- Support high-quality real-time video surveillance for security and operational management applications
- Support a cost-effective and easily managed wireless LAN architecture based on our:
  - ¬ Alcatel-Lucent OmniAccess® Wireless LAN
  - ¬ Alcatel-Lucent OmniAccess® Stellar Wireless LAN

Security is in ALE's DNA

Alcatel-Lucent Enterprise network solutions don't leave backdoors open; the code and software are independently verified and validated to ensure their integrity and security, also, the source code is deliberately varied to make it much more challenging for potential hackers.

ALE's multi-layer approach to network security allows the flexibility to incorporate secure elements into an existing network, providing enhanced cybersecurity, and then use these same components and tools to support an evolution to micro-segmented zero trust networks.

For IoT devices requesting access to the network, ALE's IoT containment strategy classifies each device based on predefined parameters in a Universal Network Profile (UNP). Based on the permissions in the UNP, IoT containment allows devices to connect to the network, but within assigned sub-segments of the network called 'containers' (or virtual networks), for an additional layer of security as a way of preventing or containing potential attacks.

ALE's industry-leading intelligent Fabric (iFab) ensures fast scalable and cost-efficient rollout of services at the edge, saving customers time and money. ALE believes that the more automation that is built into a network, and the fewer steps or systems needed to support the network, the more secure the network will be. This is true because simplicity reduces the potential for errors which can leave areas vulnerable. The ALE OmniSwitch takes simplicity to the next level.

Additionally, continuous network monitoring is essential. The network monitors behavior to ensure that the IoT devices and applications are functioning as desired. Each authorized object is stored in an inventory. This enables IT to know exactly, and instantly, how many devices are connected on the network. It is important to continuously monitor a connected object on the network to take immediate action if there is a deviation from usual behavior. In the event of unusual activity the network can take actions such as, disconnecting the faulty device, sending a notification to the network administrator, or changing the destination of the dedicated IoT container for further verification.

For ALE's network infrastructure OmniSwitch devices, independent verificationand validation (IV&V) by an independent third-party, as well as software dynamic memory diversification during each reboot have been implemented in the operating system. ALE also provides a Secure Supply Chain capability to ensure software is delivered over a secure network path only to the intended agency. These three elements combine to provide the unique ALE Secure Code solution.

ALE has also been independently certified by many international and U.S. organizations, offering JITC, NIST, FIPS, NATO, and Common Criteria security certifications. For customers concerned with the origin of the solution, ALE offers TAA (Trade Agreement Act) compliant switches.

Why Government customers choose ALE

Alcatel-Lucent OmniSwitches provide:

- **Security by default**: Remote access must be enabled by administrator
- **OS supports standards-based protocols**: Providing flexibility and investment protection
- **Network automation**: Creating an easy-to-deploy, easy-to-manage network with technologies like IoT containment and iFab
- **Licensing for features and capabilities are included**: No software licensing to track
- **JITC, NDcPP, FIPS, DOD APL approved switches**: All switches; edge, hardened, core, use the same secure level code
- **Protection from unauthorized access**: With IoT containment and iFab
- **Multi-Layer security to the device**: With macro- and microsegmentation approach to zero trust security
- **Deep Packet Inspection**: Providing application visibility and management of applications
- **Single management system**: Across the entire ALE network, providing simplicity and flexibility

Zero trust networking

Zero trust network architecture, is the next level in network architecture which operates from the premise, "Never Trust — Always Verify". This architecture can either build on an existing network security framework or it can be developed as a green-field deployment. The segmentation of a network occurs at both the macro and micro level.

In macro-segmentation, the physical network is partitioned into different logical segments. These segments can be a VLAN, a combination of VLAN + VRF, or it can also be a VPN when talking about Shortest Path Bridging (SPB), MPLS, or even VXLAN or GRE tunnels. Any traffic between users or devices on different segments is controlled by a physical firewall.

In the Alcatel-Lucent OmniSwitch and Alcatel-Lucent OmniAccess Stellar Wi-Fi, this segmentation is done dynamically – it is software-defined. When the user or device connects and authenticates, it is assigned a profile, and the profile provisions the user or device to the correct segment regardless of the physical location, switch port, or SSID.

Micro-segmentation takes things one step further. Not all users are the same, and not all users have a legitimate need to access all resources. The same profile that maps users to a segment also includes a set of policies that add even greater control over user/device privileges which may vary by roles such as HR versus Finance. This is known as role-based access, and directly relates to the principle of least privilege.

These micro-segmented devices are implemented through policies which are part of the UNP profile and dynamically applied to the device after authentication. Because neither users nor IoT devices are static (they move, connect, and disconnect) the policies cannot be tied to a location or to a port. In fact, there is a combination of factors. It starts with the identity of the user or device, but not only that, time of day, and location could all have an impact.

The combination of these factors determines the profile, and the profile determines the service, or segment. The policies included in the UNP profile, which include both security and Quality of Service (QoS) policies, determines the micro-segment. On the OmniSwitch and OmniAccess Stellar platforms, this is referred to as the User.

Alcatel-Lucent Enterprise Secure Code

With ALE, network security goes beyond required standards with:

- **Secure Code**: Provides independent third-party verification and validation source code analysis, white box, and black box testing searching for vulnerabilities in external interfaces
- **Software diversification**: ALE software implements Address Space Layout Randomization (ASLR). Each switch boot dynamically generates a unique memory layout.
- **Secured delivery of products**: For countries that require TAA. ALE provides TAA OmniSwitch models that comply with the Country of Origin (CoO) USA with all operational software loaded in a USA-based facility. Additionally specifically for US customers, the company performing the IVV testing retains the AOS code after validation testing and, over a secure connection.

Network or Access Role Profile works as a part of the IoT containment solution. It must be software- or policy-driven and not statically defined, as that would be difficult to manage.

As an example, in a legacy network the "trust" boundary is based on the point of connection: "Inside" users are implicitly trusted and "outside" users are not. Using an airport as an analogy, this would be equivalent to allowing any within-country landside passengers to go through security unchecked. With trends such as mobility and IoT, that notion of "trust" is completely outdated. For instance; a BYOD device may bring malware into the organization; an IoT device may be intrinsically vulnerable and become an attack vector; even corporate users could be malicious.

The paradigm today is zero trust. No matter where the user or device is connected, ***never trust and always verify***. Establishing identity is at the core of the zero trust paradigm. Going back to the airport analogy, the first thing a security officer will do is check the passenger's identification (such as a passport or STAR ID). Other checks such as a visa check or database check are done after the identity is established. And, since establishing identity is such a fundamental check at the core of the zero trust paradigm, next-generation networks using leading-edge solutions like Alcatel-Lucent OmniVista® Unified Policy Authentication Management (UPAM) have multiple mechanisms for determining identity. The OmniVista UPAM module is a unified access management platform for both Alcatel-Lucent OmniSwitch Ethernet switches and Alcatel-Lucent OmniAccess Stellar access points. UPAM includes both a captive portal and a RADIUS server and can implement multiple authentication methods such as MAC authentication, 802.1x authentication, and captive portal authentication.

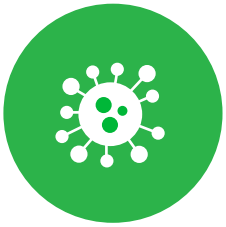
In ALE's micro-segmentation, the already established OmniSwitch network capabilities of intelligent Fabric and IoT containment allow the administrator to authenticate, classify, and monitor users and devices based on their specific roles - defined in a Universal Network Profile - not just their functional group - providing access to only the specific elements in the network required for their roles.

These key functions are an inherent part of the OmniSwitch DNA and the key to supporting zero trust networks for government agencies and departments.

Three zero trust elements

Authenticate and assign permissions

Segment



Monitor and quarantine

Check out our website or contact us.
https://www.al-enterprise.com/en/industries/government

Alcatel·Lucent Enterprise