efficient iP™ *for*

Zero Trust Security

Mixing workers on every kind of network and applications hosted in any kind of cloud requires a rethink of how the security policies are enforced. The Zero Trust approach proposes to rely on an «allow» model rather than on the standard «deny» one where users were traditionally trusted based on their location, inside considered generally as safe. In order to be able to apply this promising model it is necessary to rely on valuable and accurate data and deploy intelligent security enforcement engines.

DDI (DNS-DHCP-IPAM) solutions play an important part in making zero trust strategies successful. SOLIDserver IPAM brings its IP data lake facet of the Network Source of Truth paradigm. The DNS has granular visibility over almost all internet traffic, allowing it to offer precious contextual information for behavioral threat detection. Combining this with EfficientIP's enhanced DNS security functions and ability to filter user and application communications through the DNS engine results in DNS being your natural first line of defense.

Solution Benefits

SIMPLIFIED MICROSEGMENTATION PROCESS	using coherent IP Data Lake and network automation
BRIDGE SECURITY SILOS	share rich usage data and events with SIEM & ecosystem
ENFORCED SECURITY AT DEVICE LEVEL	DNS filtering & countermeasures based on client behavior
IMPROVED APPLICATION ACCESS CONTROL	apply DNS allow/deny policies early in the IP flow
OPERATIONAL TIME SAVINGS	automation of security workflows and processes

Business Challenges

When trying to enhance the security for users, applications and data in any organization, the fortress model is not sufficient. Protecting the perimeter of the internal network and considering anything internal is trusted and anything external isn't, does not work anymore. Zero Trust is a different approach where we consider any user or device as not safe by default. This can by extension be also applied to applications. By enforcing the «deny all traffic» rule as default security for devices on the network, the global security level is raised.

But intelligent control of network traffic or application access requires multiple security facets: 1. Visibility to correctly identify endpoints and apps. 2. Analysis of traffic intent. 3. Capability to filter the allowed traffic. Granting access is not always simple or even possible. With network perimeters blurring, the positioning of security components able to perform filtering and enforcing policy rules is not as simple as the old border checkpoint. Security must be performed at multiple layers and ideally be based on the identity of the user or the signature of the application rather than on technical attributes like IP address, MAC address or port numbers.

When filtering the access to an internal application hosted in a private cloud, we potentially cannot rely on a firewall kind of equipment to perform the screening. This is even more complex with web based applications that may rely on multiple resources from anywhere on the network, internally hosted or directly on the Internet (javascript library includes, common fonts, css, api, ...).

So how can organizations take up the interesting Zero Trust concept with a granular and phased approach, without having to redesign their entire internal IT and network security? Two standard bricks are already available in most networks and IT infrastructures to help with this: the IPAM as a repository of IP information and the DNS as a resolution service used by all components on the network.

Main Features of SOLIDserver DDI for Zero Trust

The IP address plan as the foundation of IP information: Any IT evolution is leveraging the presence of an IP network, ubiquitous, available and powerful, used for routing traffic between devices through interconnected subnets. In order to maintain this fundamental layer of any IT system, a structured IP address plan is mandatory. Managing the plan via a spreadsheet becomes impossible when trying to address multiple sites, so a dedicated IPAM solution is necessary. This can be used as the central repository for any IP-related information, and extending this with data regarding endpoints, applications or security zones allows IPAM to play a central role in security and Zero Trust as the IP data repository. Information obtained on any connecting device and any IP address used on the network can be leveraged by other security components for enforcing defined policies and protecting the infrastructure, applications and the organization's data.

DNS as the first step of the IP routing decision: any IP communication generally starts by DNS queries to transform the application or resource name into the IP address directly usable by the networking stack. Therefore the DNS is at the intent of most application traffic. This strategic position provides the DNS the ability to decide whether the client should be authorized to reach an application, based on specific criteria. In the case of Zero Trust security, a user connecting from a specific device can already provide a rich set of information on which filtering can be performed. Dividing users into groups like standard, VIP and admin enables initial filtering to determine whether they can or cannot access the app. While not strictly filtering out the traffic, it does restrict easy access to the resource, which can be considered as a first line of defense. Analyzing the requested host names and domains at the DNS level helps filtering globally. So by looking also at the requesting client, for applying different policies, means the DNS plays an essential role in the global Zero Trust rule-enforcing process.

Network segmentation for improving App Access Control: The Client Query Filtering (CQF) feature proposed by EfficientIP at the DNS recursion level helps segment network devices into multiple groups (e.g. known and unknown, trusted and untrusted) in order to offer an adapted answer to each. For every group, the policy engine embedded in the DNS can apply the appropriate security policy defined by the organization. As a simple response, the DNS may filter out resolution requests based on a threat intelligence feed composed of both external and internal sources, thus protecting against malicious domains, attack vectors and known vulnerabilities. Another technique may be to apply an «allow» filter which lists only authorized domains accessible for this set of devices or clients. This last technique is very powerful from a security standpoint and may be applied to untrusted devices (e.g. IoT) or quarantined ones during their remediation period.

Adaptive DNS countermeasure at the client level: the DNS security layer can also protect the resolution service from insider attacks. In the scope of a Zero Trust Security approach, it makes sense to mix standard filtering using threat intelligence feed, client knowledge through screening and countermeasures such as quarantining. The DNS Transaction Inspection (DTI) feature allows analysis of protocol usage and real time statistics per user in order to make advanced decisions for DNS service sake. For example, with the quarantine mode, we can authorize a device to only get DNS answers for queries already present in the cache of the DNS engine. This limits resources accessed to only those already authorized for another client. Automatically, any unexpected access during off hours would be denied. The ability to combine DNS security strategies is key for enforcing Zero Trust policies.

Rich data for security ecosystem: when setting up a Zero Trust strategy we collect data on network usages, client behavior, and application and data accesses in order to refine policies and adapt to current usages on the network. This allows leveraging of investments made on supervision platforms and the security operations center with its SIEM tooling. The DNS, as the intent of IP conversations, can provide very useful granular information. SOC efficiency is undoubtedly enhanced if SIEM tools are provided with events on specific behaviors, as they no longer need to analyze the entire traffic (e.g. DNS query and answer logs). EfficientIP DNS Guardian security solution is able to perform real time analysis of traffic thanks to it's powerful DTI inspection engine and inform, via events, an external component of the security ecosystem. The rich set of data contained in the IPAM can then be queried by the SOC to enrich the information and this event correlated with others.

Key Takeaways

IT security requires an ever evolving ecosystem of solutions, processes and skills in order to protect the organization applications and data from being altered, ciphered or stolen. DDI brings to Zero Trust security approach the ability to rely on IP networking enriched data as well as the first service touched to establish a communication- the DNS- which provides unique visibility and detection of threats before they spread.

By leveraging both valuable IP data and a service able to make decisions aligned with the organization security policies, SOLIDserver DDI helps the entire Zero Trust ecosystem to play its security role effectively.

efficient iP™

REV: C-210128

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752