Source One TECHNOLOGY

# THE SOURCE


## FIND IT, CONTROL IT

Are smart devices outsmarting your network security?
We show you how Aruba ClearPass can help your business.

### IN THIS EDITION

- Path to ClearPass
- Captive Portals
- Fewer SSIDs, Faster Wireless
- Suspect Devices
- Blocking Network Access
- Multi-Platform Environments
- Staying Off Guest Wireless
- ClearPass Integrations

**SPECIAL EDITION**
ARUBA CLEARPASS FOR ENTERPRISE

# Welcome!

**Businesses today love the idea of anywhere, anytime connectivity, but in their rush to get everything connected, often ignore the need for secure Network Access Control (NAC).**

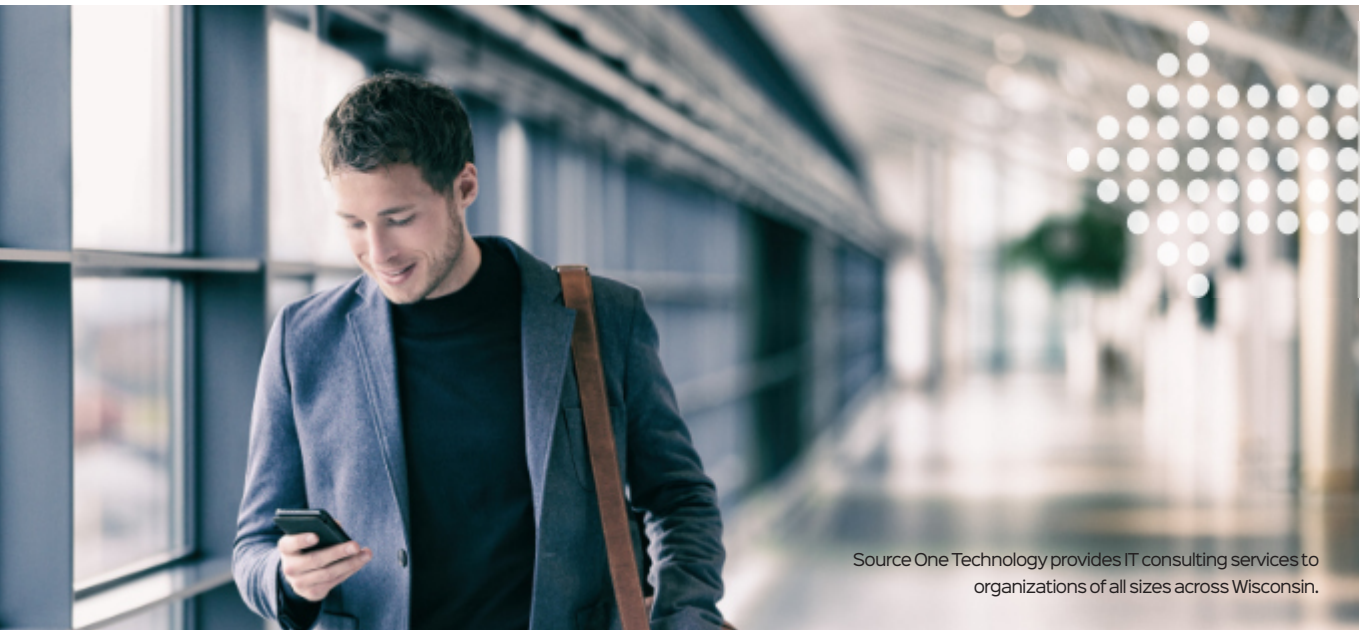
In this special edition of our free IT hints and tips magazine, we go in-depth with ClearPass from Aruba to show you how you can identify, control and respond to common network access issues and scenarios in your business.

I hope you find the magazine useful and if you have any questions check out our blog, connect with us online or give us a call.

Sincerely, Jesse.

## CONTENTS





Source One Technology provides IT consulting services to organizations of all sizes across Wisconsin.

**Jesse Rink**
PRESIDENT, SOURCE ONE TECHNOLOGY.

An experienced network engineer, Jesse has been sharing his expertise and experience with organizations across Wisconsin for over 20 years.

# A clear path to ClearPass

**If you've read previous issues of The Source, you know that we give you honest, impartial opinions on a broad range of vendors and their products. So you might be wondering why a whole edition on just one product.**

Quite simply, many organizations employ a laid-back NAC "connect now, secure later" philosophy. Others simply choose the same vendor for security that they use for network infrastructure. Both of these approaches give the illusion of security, but in reality, leave big security gaps, that enterprising users are ready to exploit.

ClearPass gives you comprehensive and precise profiling, authentication and authorization for users, systems, and devices trying to access your IT resources. It's a rock-solid, affordable solution and in our view, ideal for business.

## ClearPass is designed to address key security challenges associated with your organization by providing:

### COMPLETE VISIBILITY

When network access can be granted from almost anywhere, at any time, knowing what is on the network is the first challenge. ClearPass provides extensive discovery and profiling to enable your IT department to see who and what is connected.

### PROACTIVE CONTROL

With ClearPass Policy Manager, every user, system, and device on the network is given access to only those resources that their role requires. ClearPass authenticates every entity and assigns access privileges through policies that adjust permissions based on location, the device used, time of day, type of user and other factors.

### CLOSED-LOOP RESPONSE

Think of ClearPass as the gatekeeper of the network. The same policy engine that enables network access can be used to respond to a cyber-attack. When an alert from the security ecosystem (firewall, endpoint detection, etc.) is received, ClearPass can take a variety of policy-based actions from a re-authentication, bandwidth throttle, quarantine or block.

**Best of all, ClearPass provides all of this across multi-vendor environments (Cisco, HPE, Juniper, Palo Alto, Fortinet, etc.) so your NAC solution is not dependent on any one particular vendor.**

USE CASE

# NEVER FORGET

## A Captive Portal that remembers users!

→ PROBLEM

**Do you sometimes wish your Captive Portal could remember who people (or devices) are, so users don't have to log in to the portal every day?**

→ BACKGROUND

Many organizations use Captive Portals (from FortiGate, Palo Alto, Sophos, Lightspeed, etc.) to allow for users/devices to be authenticated for various uses such as logging and policy application. Unfortunately, the Captive Portals built into many products require periodic re-authentication. The constant need to re-authenticate can be met by resistance from employees and other end-users. Consequently, many organizations start moving unmanaged staff devices onto internal networks to remove the daily Captive Portal prompts or set up static IP addresses for devices to bypass the Captive Portal completely.

→ SOLUTION

Now just imagine for a moment, a captive portal that REMEMBERS everyone automatically and even allows them to use Google/Office 365 as their authentication source in addition to Active Directory. You won't even need to worry about having to set static/reserved IP addresses for specific users' web filtering policies either.

The username can be sent from the ClearPass captive portal to your firewall which allows you to apply different policies (such as blocking Facebook) for individual users and groups. You can even do this on your BYOD network with employee's personal devices too (ClearPass maintains a list of user devices by Mac address), so the captive portal remembers them without prompting them for login credentials every time they connect!

ClearPass resolves this problem by using a Captive Portal that permanently associates a device's MAC address with a username so that a user only has to log into a Captive Portal once from each device. The username associated with that device's MAC address can then be sent by ClearPass to your firewall every time that device connects to your network. This allows you to apply different policies (such as blocking Facebook) to individual users and groups without inconveniencing users on BYOD and Guest networks.

ClearPass provides a Captive Portal that has all the amazing benefits of your security appliance's Captive Portal -without- all the limitations.

# Ease wireless management and improve performance by minimizing the # of SSIDs

## → PROBLEM

**It's common for organizations to broadcast multiple SSIDs in their wireless environment. Each SSID is typically designated for a specific reason or function such as:**

- Employee wireless
- 802.1x based (PEAP, EAP-TLS) wireless
- Device-specific wireless (laptops and desktops, iPads, etc.)
- Guest wireless
- Or other SSIDs for a variety of other reasons

## → BACKGROUND

One thing that is often forgotten is that additional SSIDs create extra overhead and can bring even the best wireless networks to their knees.

The impact of having additional SSIDs depends on many factors but directly affects the percentage of airtime used by the 802.11 beacon frames.

Why is that important? Because 802.11 beacon frames -typically- transmit at only 1Mb/s. The more time spent sending out beacons, the less time spent on users and devices.

## → SOLUTION

Aruba ClearPass provides a solution for this!

ClearPass gives you tools to allow, or restrict, access to network resources based on nearly ANY criteria about the user, device, location, or a long list of other criteria. As an example, with a single SSID, you can still grant employees access to a set of network resources, while restricting guest users to only have access out to the internet.

These policies are defined within Aruba ClearPass based on criteria chosen in the authentication and authorization profile.

### % of Airtime used by SSID Overhead on a typical wireless environment

- Low
- Medium
- High
- Ludicrous

| No. of APs on a given channel | Number of broadcasted SSIDs: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 3.2% | 6.5% | 9.7% | 12.9% | 16.1% | 19.4% | 22.6% | 25.9% | 29.0% |
| 2 | 6.5% | 12.9% | 19.4% | 25.9% | 32.3% | 38.8% | 45.1% | 51.6% | 58.0% |
| 3 | 9.7% | 19.6% | 29.0% | 38.8% | 48.4% | 58.0% | 67.7% | 77.4% | 87.0% |
| 4 | 12.9% | 25.9% | 38.7% | 51.6% | 64.5% | 77.4% | 90.2% | 100.0% | 100.0% |
| 5 | 16.1% | 32.3% | 48.4% | 64.5% | 80.6% | 96.7% | 100.0% | 100.0% | 100.0% |

Note how SSID overhead gets significantly worse with co-channel interference. Provided by www.revolutionwifi.net.

USE CASE

# RELEASE THE HOUNDS!

## Instantly revoke network access of "suspect" devices

### PROBLEM

**Have you ever wanted to ability to instantly revoke network access for suspect devices?**

### BACKGROUND

**SCENARIO #1**

A device on your network intentionally, or unintentionally, attempts to download a virus, or exhibits behavioral patterns that are suspected by the Unified Threat Management capabilities of your Next-Generation Firewall as a possible security threat.

**SCENARIO #2**

A staff member figures out how to install TOR (a Proxy/Anonymizer program) or BitTorrent software on an office PC, company tablet, or attempts to run the offending software from a personal device.

Wouldn't the next logical step be to automatically disable network access for the offending device immediately, to maintain the overall integrity of your network?

### SOLUTION

ClearPass can easily revoke network access for suspect devices without requiring you to track down the device itself. The entire process is automated, regardless of whether the device is wired directly into your wireless or wireless.

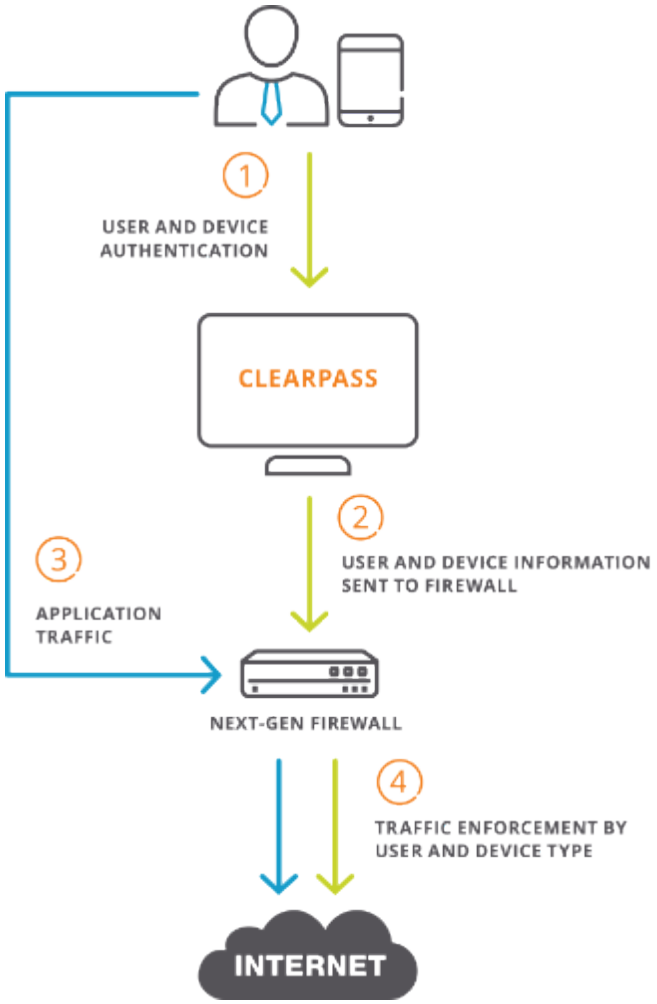
One of the great things about ClearPass is that it has the capability to receive NGFW/IPS events and communication from your Next-Generation firewall.

ClearPass accomplishes this through various means, including methods such as; Syslog messaging, SNMP trap reporting, etc. that trigger a RADIUS CoA (Change of Authorization) which results in the suspected device having its network access quarantined or completely revoked, immediately!

Furthermore, the CoA can then be followed up with an email alert sent to the appropriate network administrator so proper remediation steps can be taken with the device in question.

USE CASE

# Block network access if users abuse network privileges



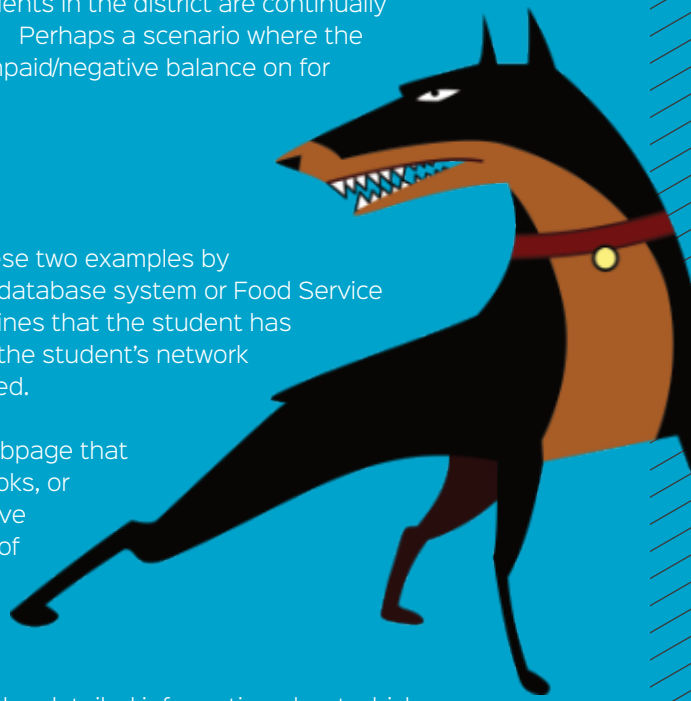

AN EXAMPLE OF ENHANCED POLICY ENFORCEMENT.

## PROBLEM

**Have you ever wished that you could block access for a user because of inappropriate usage of technology?**

## BACKGROUND

Imagine in a school environment where students in the district are continually late paying fees or fines they have incurred. Perhaps a scenario where the student has overdue Library books, or an unpaid/negative balance on for their Food Service account.



## SOLUTION

ClearPass can be configured to allow for these two examples by running custom queries against the Library database system or Food Service database system, and if the system determines that the student has overdue books or has delinquent balances, the student's network access and privileges can be limited or denied.

The student can even be redirected to a webpage that asks them to return their overdue library books, or make a payment to catch up on their negative balance. There are an almost unlimited set of criteria for blocking network access if a student abuses their privileges.

Keep in mind that ClearPass can also trigger an email to your Helpdesk that provides detailed information about which device had its' access blocked, when it happened, and the reason why, helping to keep your IT support staff informed and aware!

USE CASE

# Aruba ClearPass in multi-platform environments

## PROBLEM

**You want to use ClearPass to manage your guests, BYOD, and company-owned device wired and wireless access, but you are using a firewall from one vendor, a switch from another, and a wireless controller or access points from a third vendor.**

## BACKGROUND

In many scenarios, selecting the best product for your needs typically results in an environment that includes different vendors for each of your core products.

Those products are often fairly unaware of each other or have read-only access to each other.

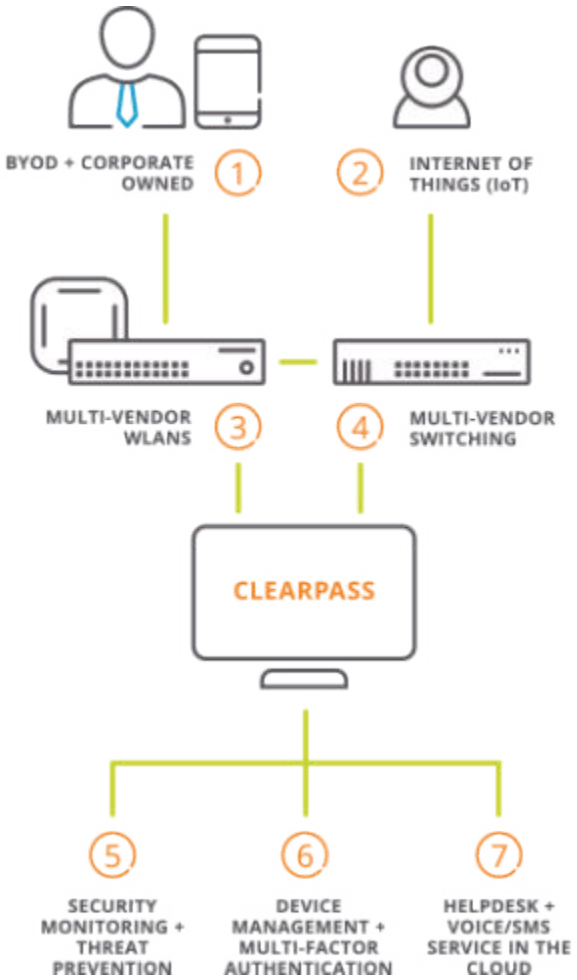
## SOLUTION

ClearPass provides a central location for network access control event logging and coordination across -ALL- of your infrastructure.

If you have Palo Alto firewalls, HPE Aruba switches, Cisco wireless, and ServiceNow for your ITSM (IT Service Management), ClearPass has direct integration with all of those products and can set up Service Chaining such that ClearPass can facilitate two-way communications that generate all of the appropriate actions.

Consider an example where your firewall sees malware downloading to an endpoint device. The firewall can report the threat to ClearPass which allows ClearPass to tell your HPE Aruba switch, or Cisco wireless, to disconnect or quarantine the device! Furthermore, ClearPass can then create a helpdesk ticket so when that offending user calls in for support, they are not trying to find out which product is causing the problem - your IT team will already have a service ticket with “actionable” information.

ClearPass provides a way to make all of your infrastructure work together to solve real problems.



USE CASES

# THIS IS NOT THE WIFI YOU'RE LOOKING FOR

## Force company devices to stay OFF the guest wireless network

'Obi-Wan' by Stanley Chow - stanleychowillustration.com

### PROBLEM

**How many times have you found staff devices incorrectly connected to the Guest Wireless network instead of the preferred secured wireless network?**

### BACKGROUND

This scenario is often encountered when mobile devices such as iPads, Chromebooks, etc. are allowed to travel off-site/home with the staff member and the user needs the ability to join the device to a foreign SSID (such as their wireless network at home). Unfortunately, when those same devices come back to the office, the user may incorrectly connect to the Guest Wireless network (intentionally, or unintentionally) which may break certainly functionality for that since the device cannot communicate properly to internal resources/ network (due to ACL restrictions in place), and can even have limited performance due to possible bandwidth restrictions placed on the Guest Wireless network.

### SOLUTION

You can take advantage of ClearPass to keep company owned devices off your Guest Wireless network!

ClearPass can keep devices off the guest wireless in a variety of ways, such as by integrating with Active Directory or Google Admin to determine if a device is a company-owned device, but another even simpler method - Zero-Touch! - is to configure ClearPass so that any device that has previously joined a non-Guest wireless network (such as during MDM/ Enterprise Enrollment, post-OS deployment with Windows, etc.) has a special “Attribute” applied to it, which indicates the device cannot connect to the Guest wireless in the future.

Now your company-owned devices will be forced to stay off the Guest Wireless network, and all with Zero-Touch administration!

# CLEARPASS

**works with your existing technology vendors***

## UEM, ENDPOINT AND NETWORK SECURITY

| | | | | |
|---|---|---|---|---|
| Symantec | CYLANCE | DELL | citrix | f5 |
| FORTINET | IBM | jamf | JUNIPER NETWORKS | McAfee |
| mobileiron | paloalto NETWORKS | SAP | FIREEYE | tenable |

## IDENTITY PROVIDERS

| | | | |
|---|---|---|---|
| amazon | box | | GitHub |
| LinkedIn | salesforce | okta | |

## SMS

| |
|---|
| Clickatell |
| twilio |

## CLOUD SERVICES

| | | | |
|---|---|---|---|
| Microsoft | PagerDuty | Google | slack |

* A small sample of partners.

# What we do

**We help you get the most out of your investment in technology**

## Business management

Business accounting software – Quickbooks. Peachtree.

Virtual CIO – Helping you create and implement the right IT strategy for your organization.

## Communication and collaboration

Business email – Office 365 and Google Workspace solutions.

## Cybersecurity and business continuity

Data backup – Local. offsite and hybrid business continuity and disaster recovery solutions for servers and SaaS.

Disaster recovery planning – Helping you take back control in the event of a disruptive event with a clear. actionable plan.

Endpoint security – Installing. configuring. and maintaining endpoint protection.

Incident response – Addressing and managing the aftermath of a security breach or cyberattack.

IT assessments – Offering vulnerability management. penetration testing. risk assessment. security awareness training and compliance consulting services.

Security awareness training - Protecting your staff and organization from malicious behavior using reputable programs from KnowBe4 and Proofpoint.

## Desktop support services

Apple support – Installing. configuring. and optimizing macOS and iOS devices. and MacPractice software.

PC and printer support – Managing the entire desktop lifecycle from procurement. deployment and support through to disposal.

## Digital transformation and cloud migration

Migrate services to Azure and AWS – Microsoft Azure and Amazon AWS public/hybrid cloud solutions.

Remote access/work from home – Site-to-Site VPNs. PPTP/IPSec VPNS. SSL VPNs. Terminal Services.

## IT infrastructure services

Firewall and network security – Protecting your organization from risks and vulnerabilities.

IT performance monitoring – Making sure your environment is healthy and performing as expected.

Networking support – Providing the switching and routing backbone and highway for your devices.

Server administration – Windows 2012. 2016. 2019. 2022. Linux and Mac.

Storage and SANs – Design. build and manage your infrastructure across different vendor platforms.

Virtualization – VMware vSphere. Microsoft Hyper-V virtualization solutions.

No sales people

16+ years experience

98% retention

No long-term contracts

# WHAT NOW?

**If you'd like to find out more about Aruba ClearPass and how it can be used to improve your network security, get in touch!**

> **We use Source One Technology for network support as well as other unique situations that arise. Their integrity, thoroughness, and ability to adapt are what impress us. We thoroughly trust Source One Technology to provide high-level service in support of our technology, and we would not hesitate to recommend them to others for technology support and implementation**
>
> Pat Foran
> VP OF INFORMATION TECHNOLOGY
> **BANK OF DEERFIELD**

See what our customers are saying about us
sourceonetechnology.com/testimonials

Source One TECHNOLOGY

Call us on (262) 432 9000 or visit www.sourceonetechnology.com
333 Bishops Way, Suite 120, Brookfield, WI 53005