# **Identity Aware Proxy**



# The Evolution of Today's Security Architectures

**Presented by** 

Jason Wilburn Solutions Engineer

## What is Zero Trust?

A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet).

NIST

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
  - Network locality is not sufficient for deciding trust in a network.
- Every device, user, and network flow is authenticated and authorized.
- Policies must be dynamic and calculated from as many sources of data as possible.

#### Zero Trust is a data-first framework to achieve security using microperimeters and microsegmentation.

Forrester

Zero trust networking is a concept for secure network connectivity where the initial security posture has no implicit trust between different entities, regardless of whether they are inside or outside of the enterprise perimeter. Least-privilege access to networked capabilities is dynamically extended only after an assessment of the identity of the entity, the system and the context.

### Gillman and Barth

Gartner









#### Today's Architecture PaaS laaS Multi-Cloud Everything **Security Stack** Else SaaS % Our Controlled Comfort Zone DMZ PaaS laaS Cloud **Security Stack** Perimeter SaaS **Security Stack** % % External Partners Internal Core Routing Data Center Data Center Security Stack Applications **Corporate Enterprise HQ** Site **Remote Sites**

# Today's Architecture



### Tomorrow's Architecture



# **(C)** Identity Aware Proxy (IAP)







• Firewall

- Anti-Virus
- Patch Management
- Machine Certificate
- Hard Disk Encryption
- File
- Process
- Public File Sharing





<b>(5</b> )	<pre>clactype html PUBLIC "-//IETF//DTD HTML//EN"&gt;                             </pre>
Secure Logon for F5 Networks	<pre> </pre>
Username user1	<pre>&gt; <tale id="page_header">. &gt; . &gt;</tale></pre>
Password	<pre>▼ ▼ ▼</pre>
Logon Click here if already logged in	<pre>v(d id="main_table_info_cell"&gt;     v<form action="/     subsession_logon_submit.php3?state=000ffff5f7a80be" autocomplete="off" id="auth_form" method="post" name="ell" onsubmit="javascript: return masterSubmit(this);"></form></pre>
	<pre>v v </pre>
	<pre>v(tr&gt; v(tr&gt; v(td colspan="2" class="credentials_table_unified_cell"&gt; v(td colspan="2" class="credentials_table_unified_cell"&gt; v(td colspan="2" id="label_input_2"&gt;Password(/label&gt;</pre>
	<input autocapitalize="off" autocomplete="off" class="credentials_input_password" form="&lt;br" id="input_2" type="text" value=""/> "auth_form" data_biai="assword" value id="input_2" autocomplete="off" autocapitalize="off" form=
	<input name="08e73f4ad3081800ec4950604aa9eb6d9343f5ea594ea9d6fc1c49645f085d3b" type="hidden" value="08e73f4ad3011800622a093e7d3439595d192049cfaf8f8317e30346c3277283aeb2d0c4e6eeb0de44692bd63741c934ea6c49a28bf8837fc0a: 9cc90a440685675516ba464f755204c93c9f6f82f7428c6f0d8a31b4043936659c2cae3d2a8b83316dbccf6c52f1275e777c3c847f00883384afc1 37688f378fa447eb6ff"/>





### • Per-Request Policies using Visual Policy Editor

Per-Request Policy: /Com	AP_DEMO.app/IAP_DEMO_perRequestPolicy Edit Endings (Kedings Allow, Reject (editud))	
Start Malack +-		
UBL Braching	1         100000 + ++)         1000000 + ++)         1000000 + ++)         1000000 + ++)           1         ++         1000000000000000000000000000000000000	Allow  Reject  Reject  Reject  Reject  Reject  Reject  Reject  Reject  Reject  Reject

### Identity Aware Proxy Guided Configuration



Delivers secure access to applications based on the principle of "Never Trust, Always

Identity Aware Proxy Provide secure access to public applications based on realtime device posture, user identity, and step-up authentication.





#### Configuration Name

IAP\_DEMO Type a name for this guided configuration.

Enable F5 Client Posture Check 0

#### CA Trust Certificate 0

ca.f5lab.local.crt	~	2

Posture Settings

Name

FW\_CHECK

Allow Unsigned Client Posture Data 0

A When you select Allow Unsigned Client Posture Data, your system and data are vulnerable to DoS and IP spoofing attacks.

#### Platforms

Windows
Select Browsers: 2 Chrome 2 Firefox 2 Edge
Client Side Checks 0
Antivirus
Firewall     Hard Disk Encryption     Public File Share     Patch Management
Domain Managed Devices
Domain Name 🚯
f5lab.local
2 macOS
Select Browsers: 2 Chrome 2 Firefox
Client Side Checks 0
Antivirus
Firewall Hard Disk Encryption Public File Share Patch Management

Domain Managed Devices ()



Virtual Server

#### Virtual Server O Create New O Use Existing

#### Destination Address 0

#### O Host O Address List

10.1.10.100

Service Port 0		
443	HTTPS	~

#### Enable Redirect Port

Select to specify port for redirecting traffic to the Service Port.

#### Redirect Port



Client SSL Profile Create new Use Existing

Client SSL Certificate 0

acme.com-wildcard.crt

acme.com-wildcard.key 🗸 🗸

Trusted Certificate Authorities for Client Authentication () ca.f5lab.local.crt ~ 2

#### Server SSL Profile 0

Create new OUse Existing

Available		Selected
Filter		Common
Common		serverssl
adapi.f5lab.local	00	
apm-default-serverssl		
Create Profile in BIG-IP UI		

#### iRules 0

Available		Selected
Filter		
Common	000	
_sys_APM_activesync		
_sys_APM_ExchangeSupport_helper	(W)	
_sys_APM_ExchangeSupport_main		

### User Identities

- Active Directory
- LDAP
- RADIUS
- HTTP
- SAML
- CRDLP
- OCSP
- OAuth

#### **Authentication Properties**

Authentication Properties

Service Provider Properties

Authentication Type 0

SAML

Entity ID 0

Scheme 0

https

Name

me	
hentication Type 0	
AAA	~
Active Directory	~
Active Directory	~
Active Directory	
Active Directory Trusted Domain	
LDAP	
RADIUS	
HTTP	

 $\sim$ 

 $\sim$ 

Host 0

# Authentication Properties Name Authentication Type On-Demand Certificate Authentication

#### **Choose Authentication Server Type**

CRLDP	~
CRLDP	
OCSP Responder	
Select	~

#### Authentication Properties

Name	
Authentication Type ()	

#### **OAuth Properties**

Choose DNS Resolver
---------------------



#### At least one provider is needed





MFA





# SSO & HTTP Header

#### Single Sign-On Settings & HTTP Header Properties

	_		_	_
N	а	n	٦.	Δ
	а			c

Specify the na	ame of the SSO confi	guration.		
Туре 🚯				
<ul> <li>Single S</li> </ul>	ign-on Method	HTTP Headers		
HTTP B				
	0000			
HTTP B	HTTP Basic			
Kerbero	Kerberos			
NTLMV	NTLMV2			
OAuth Bearer				
Cancel	Save			

#### Single Sign-On Settings & HTTP Header Properties

Name		
Specify the name of the SSO configuration.		
Type 0		

Single Sign-on Method O HTTP Headers

SSO Headers 0			
Header Operation		Header Name	Header Value
replace	~	Authorization	%{session.sso.token.last.username}

Cancel Save



### Applications

#### **Application Properties**

N	ame 0
	header-iap.acme.com

#### FQDN 🛈

header-iap.acme.com

#### Subpath Pattern 0

/admin.php

#### Pool Configuration

Health Monitors 0

Available	Selected
Filter	
/Common/gateway_icmp	
/Common/http	
/Common/http_head_f5	

+

#### Load Balancing Method 0

Round Robin

Y

IP Address/Node name 1	Port	Connection Limit	Priority Group
10.1.20.6	443 HTTPS ~	O	0



Application Groups

scription 0			
olications List 0			
Available		Selected	
Filter	Т	header-iap.acme.com	
basic-iap.acme.com		/admin.php	

Cancel Save

Application Group Properties



Contextual

Access

#### **Contextual Access Properties**



#### Enable Additional Checks ①

#### Trigger Rules

Trigger rules are executed in the order they appear. If trigger rules are not defined, then the default fallback rule is executed.

Add Delete		Items: 1	Filter Type by Name
Name	Trigger Types	Match Action	Sequence
get-user-status	HTTP Connector Request <b>()</b>	Step Up	
Default Fallback 🚯		Reject ~	

Cancel Save



Contextual Access (Triggers)

#### Contextual Access Properties > Trigger > New

Name	
Trigger_Rule-1001	
□ IP Geolocation 0	
□ HTTP Methods 0	
□ IP Reputation	
□ IP Address Changed 0	
Device Posture Check 0	
Client Posture Information 0	
HTTP Connector Request	
🕗 User Group Check 🚯	
User group check is using the subsession.ad.last.attr.memberOf user group source session variable in ad primary authentication.	
Select Groups	
Primary Authentication : ad   Server : prebuilit-ad-servers	

	Items: 66		
Refresh		Filter by Group Name	
Group Name	Group DN	Action	
Access Control Assistance Opera	k CN=Access Control Assistance Operators, CN=Builtin, DC=f5lab, DC=local	Add	
Account Operators	CN=Account Operators,CN=Builtin,DC=f5lab,DC=local	Add	
Administrators	CN=Administrators,CN=Builtin,DC=f5lab,DC=local	Add	
Allowed RODC Password Replica	ti CN=Allowed RODC Password Replication Group,CN=Users,DC=f5lab,DC=local	Add	
Backup Operators	CN=Backup Operators,CN=Builtin,DC=f5lab,DC=local	Add	
Cert Publishers	CN=Cert Publishers,CN=Users,DC=f5lab,DC=local	Add	
Certificate Service DCOM Access	CN=Certificate Service DCOM Access,CN=Builtin,DC=f5lab,DC=local	Add	
Cloneable Domain Controllers	CN=Cloneable Domain Controllers,CN=Users,DC=f5lab,DC=local	Add	
CreateUser	CN=CreateUser,OU=IT,DC=f5lab,DC=local	Add	
	500		1 - 66 of 66 items

#### Selected User Groups 0

All O Any O Not Matching Any

Operation	Groups	Act	tio	n	
Equals ~		+		×	

#### Match Action 0



Cancel Save



#### Logon Page

Form Header Text

Secure Logon <br> for F5 Networks

Type the text to display for the form header.

#### Logon Page Input Field #1

Type the text to display for the first field on the logon page. Usually, it's Username.

#### Logon Page Input Field #2

Password

Type the text to display for the second field on the logon page. Usually, it's Password.

#### Logon Button

This is the label for the logon button. It defaults to Logon.

#### **Remediation Page**

Software download URL 0

https://iap1.acme.com/epi/downloads

#### Error Messages

Customization

Invalid client data 0

Endpoint Inspection error. Please contact your system administrator for assistance.

#### Network Firewall check failed 0

Network Firewall check failed.

Antivirus software check failed 0

Antivirus software check failed.

#### Patch management check failed 0

Patch management check failed.

#### Hard disk encryption check failed 0

Hard disk encryption check failed.

#### File check failed 0

File check failed.

Health Agent check failed 
Health Agent check failed.

#### There are pending changes for your application.

The pending changes to your application are ready to be deployed. Review the summary. You can click 🖋 on any step to make changes.

#### Objects 🕨

#### Summary

<b>A</b> ==	Le Device Posture ▼		(M <sup>2</sup>
	Enable F5 Client Yes Posture Check		
	CA Trust Certificate /Common/ca.f5lab.local.crt		
	Posture Settings		
	Name	Selected Platforms	
	FW_CHECK	Windows, MacOS, iOS, Android	
0	Virtual Server		ø
:::: ::::	User Identity >		Ø
0	MFA →		<b>A</b>
٩,	SSO & HTTP Header >		di s
	Applications >		ø
Ð	Application Groups >		ø
	Contextual Access		Ø
ŧ	Customization >		Ø
U	Logon Protection >		Ø
Cance	Save Draft Back Deploy Undeploy		





# LAB TIME

