

Deploying a SAML-Based Single Sign On Solution *(using Ping Federate)*

Bruce E. Wilson
Enterprise Architect
Oak Ridge National Laboratory
wilsonbe@ornl.gov
@usethedata

Outline

- What is SAML?
- How does SAML Work?
 - Integration with Kerberos SSO
- Setting up and debugging
- SAML and Federation
- Security

Questions? Ask as we go along.

What is SAML?

- Complicated
- Security Assertion Markup Language (2.0)
- SOAP, XML, and PKI based
- Token Bearer most common
 - Browser based, relies on 301 redirects
- Artifact Binding more secure, but tradeoffs
- Enhanced Client or Proxy (ECP) not widely supported but can work with ssh

SAML Terms

- Identity Provider (IdP)
 - User interacts with this to prove who they are
 - Makes the Identity Assertion
 - Provides Attributes about the identity
- Service Provider (SP) (aka Relying Party)
 - The thing the user wants to use
 - Trusts one or more IdPs

Selected SAML Toolsets

- ADFS (Microsoft)
- Shibboleth (Internet2, open source)
- Ping Federate (Ping Identity)
- Okta (Identity as a Service – IDaaS)
- SimpleSAMLphp (open source)
- mod_auth_mellon (open source, for Apache)

SAML Response: Key Elements

- Audience (which SP, and for how long)
 - Valid for one SP, typically 2-5 minutes
- Signed with IdP private key
 - Critical for security
- Can be encrypted with SP Public Key
- Unsolicited vs SP Initiated
- SAML_SUBJECT, zero or more attributes
 - Email and PseudOID most common
- RelayState – tool for SP to manage state
 - Typically a nonce, for privacy; separate parameter

Ugh

```
<samlp:Response Version="2.0" ID="Abk6S5cOPT.cmtI5OZZ6yWpcANX" IssueInstant="2016-07-30T13:32:05.991Z"
InResponseTo="bfbe499f6efbf4820c437cc6cb51a9a4" Destination="https://dmptool.org/Shibboleth.sso/SAML2/POST"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" > <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.ornl.gov/idp</saml:Issuer> <ds:Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> <ds:SignedInfo> <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /> <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" /> <ds:Reference URI="#Abk6S5cOPT.cmtI5OZZ6yWpcANX"> <ds:Transforms> <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" /> <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" /> </ds:Transforms> <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmldig#sha256" /> <ds:DigestValue>FGJqz18CGSccmgZCgFyfL5YDjbjNcCEnTbBEyqgBk5A=</ds:DigestValue>
</ds:Reference> <ds:SignedInfo> <ds:SignatureValue> g3/yfdvwUC+cJe1mwDUKwM8TQf1bcwwP6shNPEuEBjRbe1jS9IkERItcxZVe+sH7bytFIEAO8KkF
VJFEgSinQD6cJXj2Kw7I9YHRAjvgDrn5e7Hd8/Bg4EEVbOCbjXmpCTGmIwZwp0i8+bzKJxXkJyJuY
e4p9tVVOMrXb7OHzxPbCThat8cYZjrfQpByDY9NRhfcMSqOhsQMXzUNDHWImTpXGs1IuiDAf6UU
1CyG4KEt811HEydRuUF91U+YmaGG9L5hjx8j/KmAMDppL46bcUk/etc1F+Z4nF735tdmC2pjoytj fOp8VU2VnqBk4JbpgEui92300tr6qGqujSCKUw==
</ds:SignatureValue> <ds:KeyInfo> <ds:X509Data> <ds:X509Certificate>
MIIDfDCCAmSgAwIBAgIGAUiANDwoMA0GCSqGS1b3DQEBBQUAMH8xCzAJBgNVBAYTA1VTMQswCQYD
VQQIEwJUTjESMBAGa1UEBxMjT2FrIFJpZGd1MSYwJAYDVQQKEx1PYWsgUmlkZ2UgTmF0aW9uYWwg
TGFib3JhdG9yeTENMASGA1UECxMESVRTRDEYMBGA1UEAxMPZXh0aWRwLn9ybnuwZ292MB4XDTE0
MDKxNjIwNDMwMFoXDTE3MDkxNTIwNDMwMFowfzElMAk1UEBhMCVVMxCzAJBgNVBAGTA1ROMRIw
EAYDVQQHEw1PYWsgUmlkZ2UxJjAkBgNVBAoTHU9hayBsaWRnzsBOYXRpb25hbCBMYWJvcnF0b3J5
MQ0wCwYDVQQLewRJVFNEMRgwFgYDVQDEw91eHRpZHAub3JubC5hb3YwggEiMA0GCSqGS1b3DQE
AQUAA1BDwAwgeEKAOIBAQCFSeoVvS5n9QKGQNZXCLwoTLnxCs7BqUguHiFlgt0FUOocyBX08Hnh
/BCsUXgRIT1RgYf9f1qsn0Qiw+jccSx0KRnL4vEmLql10AWv0bpJMB0vptqt+hbfKzFecor+Kv
Tx4r9sB+wRofHWXZUuI0eBLHbtxmEarLCpdKaGCiNH5hLDWVQzSERMbMtndLoad BalanceremY/oVs8ADhz05kQ
ilvM0WqE+br690Qb3kWeoSAUXIq+tMqGO3GvhFDQ7nNZDZrsZnwKJ/dnrdFeimnfQmfUUHGdNUJI
conIR69rHEeH0+8A068tv312wkqZ7RB5mU/Jjn4cd1QxYayEW1D1Kq5nEhFHAqgMBAEwDQYJKoZI
hvcNAQEFBQADggEBAHfvahW8rwe5KVkY67yk36KvX32YzREBEXFTP6RDraKW+V4fxmIcZ8aIAJRfa
maSpdkVny1lmcauuDXJB2ZsJrvQSU2v4jxZmDlo2CGjhNlxgKwxhmlAxLVH/jjHpw17KC2QCJ
F4WIIIC8ait0YTevmE4uUszztd+NRN41YzPg+gfDx+ogxKhs74DyX7rKZt1D0Dv0EWw5t48uT5
PasMG0XKPy4PjPfLkkNA/hg2ZntUCgv0CxI9xa1hcJnVtRSleEe1TW/BXu0IhjDzxC6B21IC67hh wunAENI37gwDHLVT688gsIa+tB+uMKv/0yZi5AlnZqsJlhbujJxPM10=
</ds:X509Certificate> </ds:X509Data> </ds:KeyInfo> </ds:Signature> <samlp:Status> <samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success" /> </samlp:Status> <saml:Assertion ID="eZmUQ--.94WLAMTDRkOm4lvtJYQ"
IssueInstant="2016-07-30T13:32:05.998Z" Version="2.0" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" >
<saml:Issuer>https://idp.ornl.gov/idp</saml:Issuer> <saml:Subject> <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">wilsonbe@ornl.gov</saml:NameID> <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData Recipient="https://dmptool.org/Shibboleth.sso/SAML2/POST" NotOnOrAfter="2016-07-30T14:07:05.998Z"
InResponseTo="bfbe499f6efbf4820c437cc6cb51a9a4" /> </saml:SubjectConfirmation> </saml:Subject> <saml:Conditions NotBefore="2016-07-30T13:27:05.998Z" NotOnOrAfter="2016-07-30T14:07:05.998Z" > <saml:AudienceRestriction>
<saml:Audience>https://dmp.cdlib.org</saml:Audience> </saml:AudienceRestriction> </saml:Conditions> <saml:AuthnStatement
SessionIndex="eZmUQ--.94WLAMTDRkOm4lvtJYQ" AuthnInstant="2016-07-30T13:32:05.998Z" > <saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef> </saml:AuthnContext>
</saml:AuthnStatement> <saml:AttributeStatement> <saml:Attribute Name="urn:mace:dir:attribute-def:displayName"
NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >Wilson, Bruce
E</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="urn:oid:0.9.2342.19200300.100.1.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>wilsonbe@ornl.gov</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="urn:oid:2.16.840.1.113730.3.1.241"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" >Wilson, Bruce
E</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>wilsonbe@ornl.gov</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="urn:mace:dir:attribute-def:eduPersonPrincipalName"
NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>wilsonbe@ornl.gov</saml:AttributeValue> </saml:Attribute> <saml:Attribute Name="urn:mace:dir:attribute-def:mail"
NameFormat="urn:mace:shibboleth:1.0:attributeNamespace:uri" > <saml:AttributeValue xsi:type="xs:string"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
>wilsonbe@ornl.gov</saml:AttributeValue> </saml:Attribute> </saml:AttributeStatement> </saml:Assertion> </samlp:Response>
```

ORNL SAML: High Level

ORNL DMZ



Ldap

extidp03 (OSTI)



extidp01 (5600)

Load Balancer



User Device (browser)

Internet



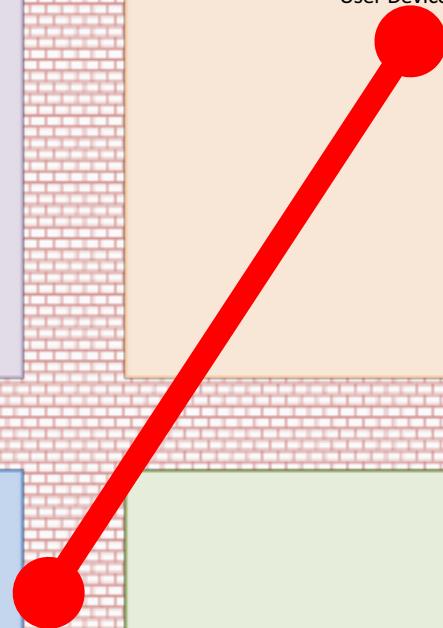
DCs

intidp03 (OSTI)



intidp01 (5600)

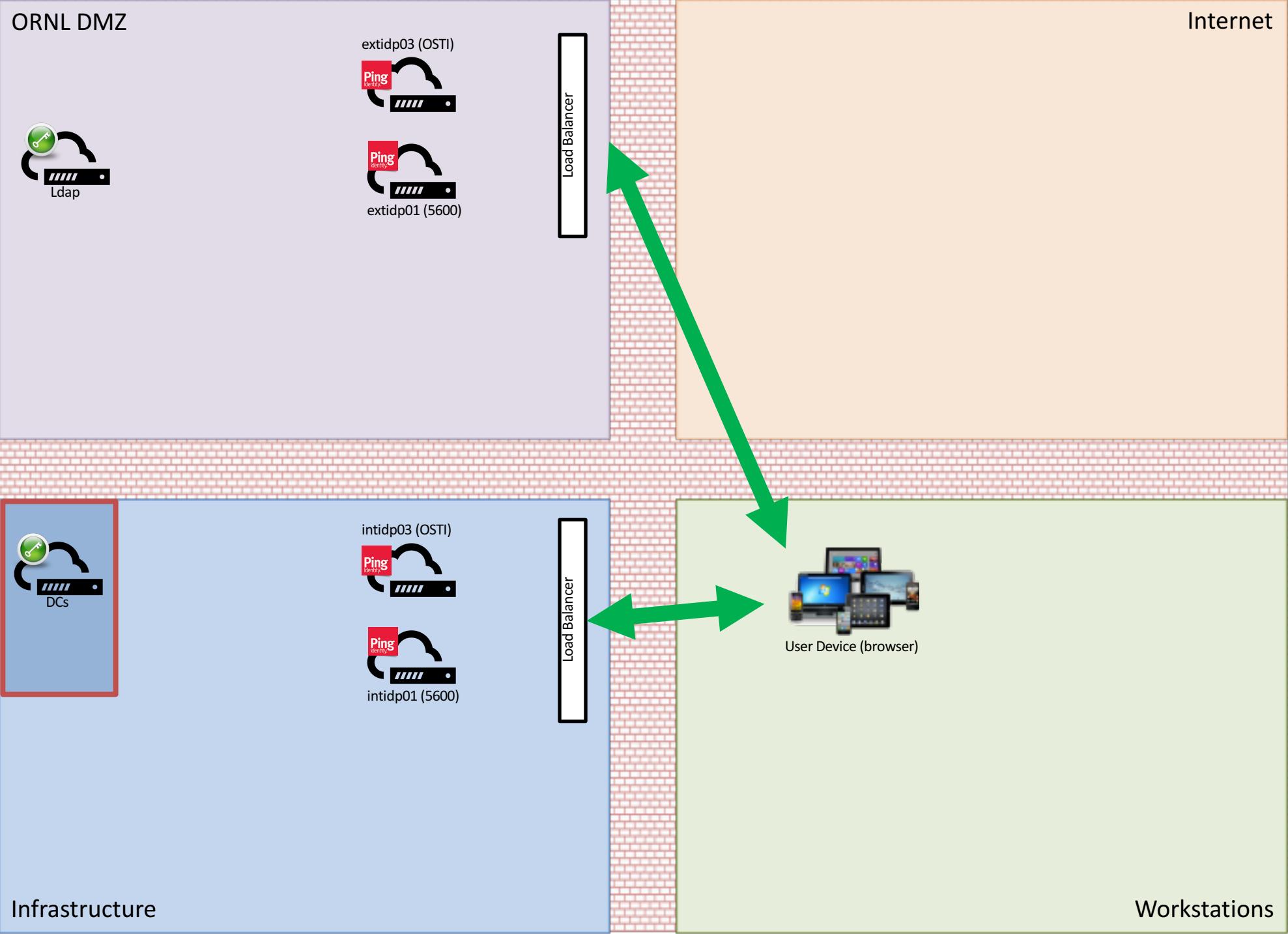
Load Balancer



Infrastructure

Workstations

ORNL SAML: High Level



ORNL SAML: Mostly Linux (RHEL 6 -> RHEL 7)

ORNL DMZ



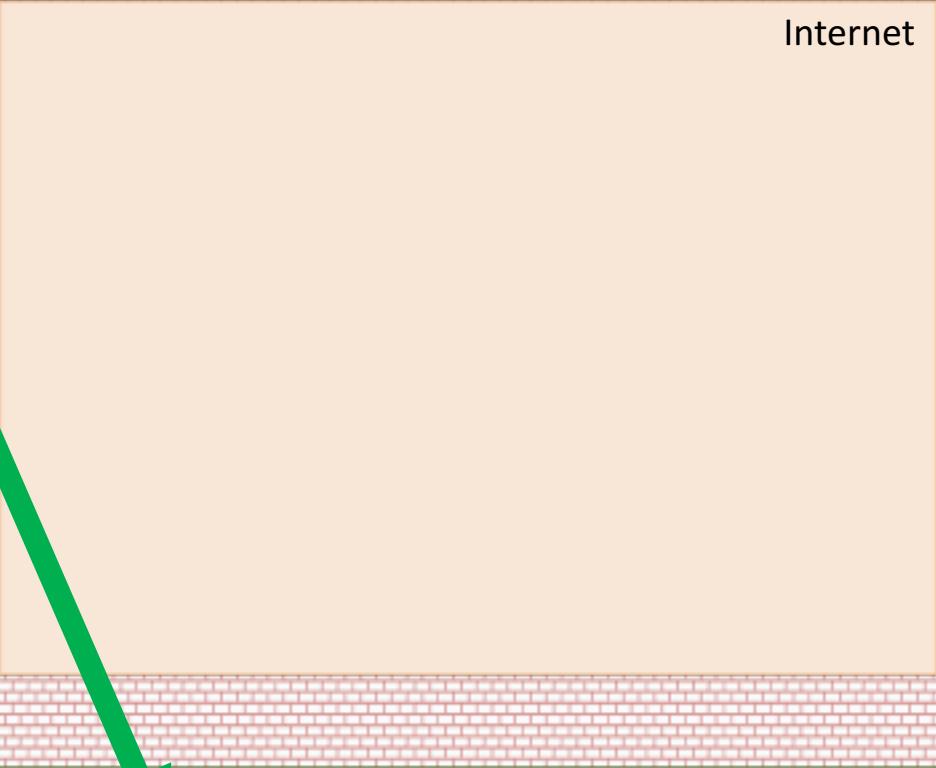
extidp03 (OSTI)



extidp01 (5600)

Load Balancer

Internet

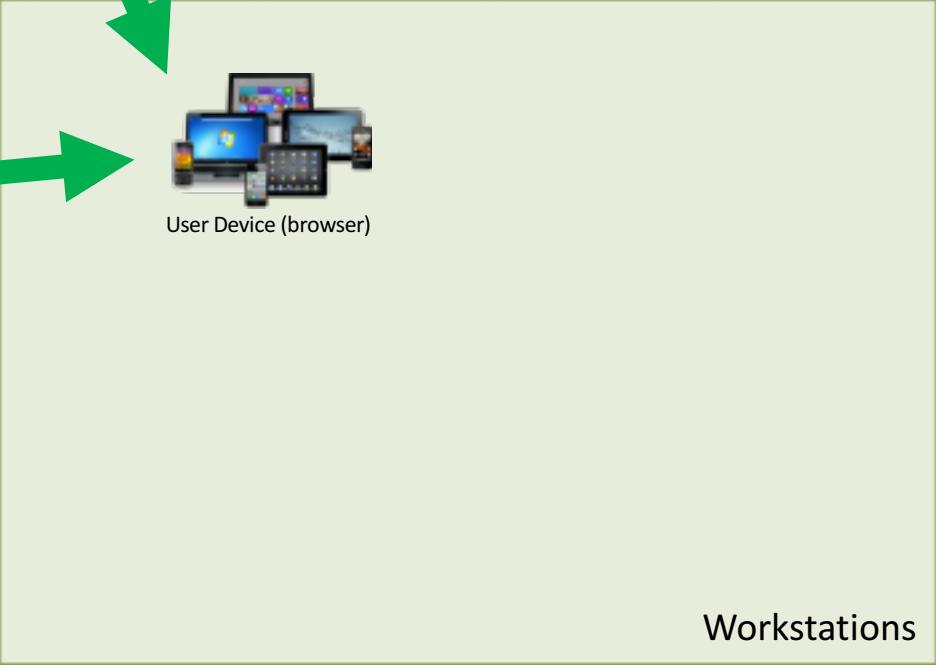


intidp03 (OSTI)



intidp01 (5600)

Load Balancer



User Device (browser)

Windows. Isolated in its own network box. Life is better that way 😊

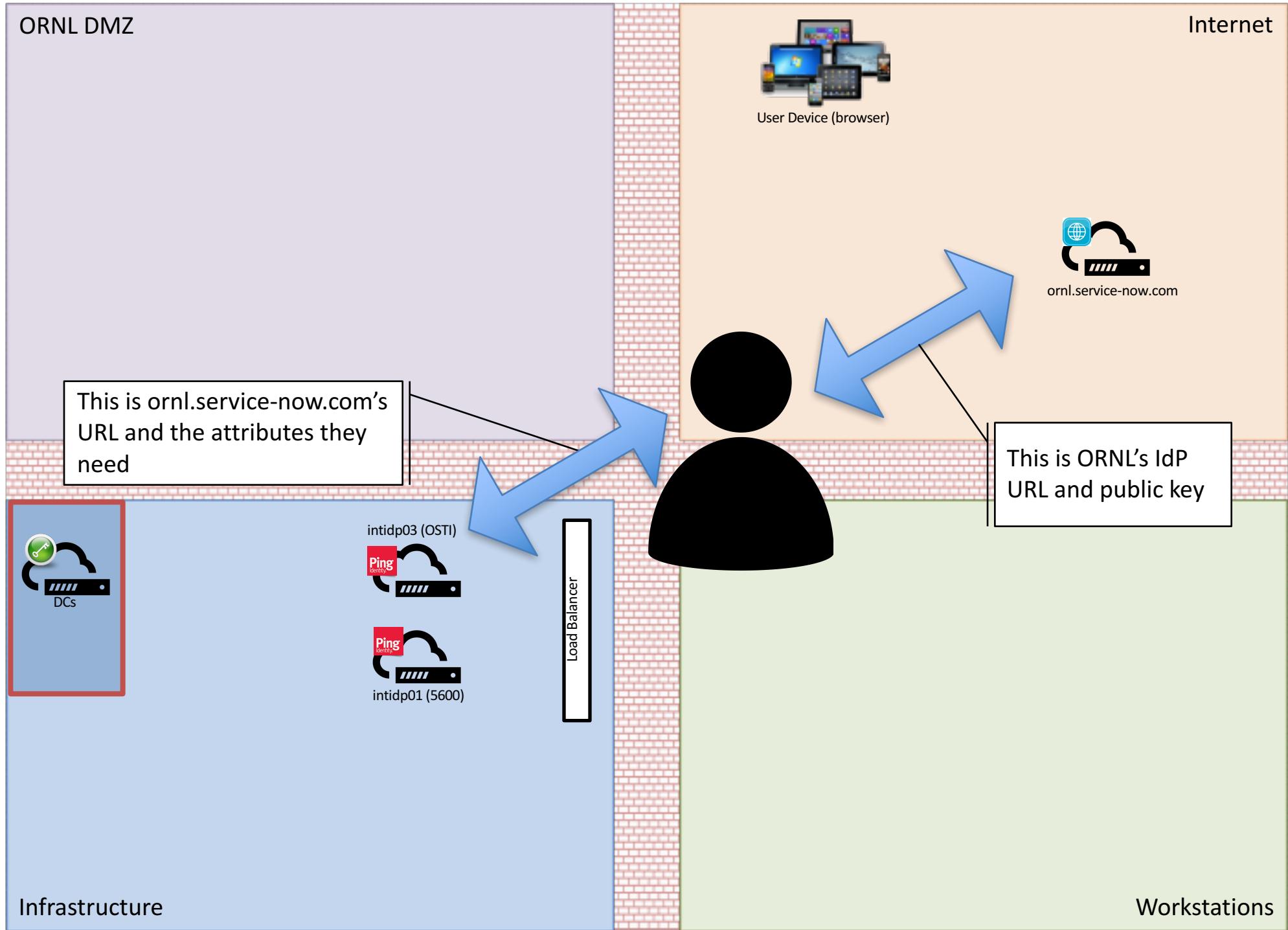
Infrastructure

Workstations

An Example: Service Now

- Cloud Service Provider
- Use ORNL accounts, but don't send password
- Accessible only from the ORNL network
- Want to use Kerberos SSO if available
 - Minimize password use, leverage MFA

Ping Fed and Service Now: Set up Connection



Ping Fed and AD: Set up Kerberos

ORNL DMZ

Internet



User Device (browser)



ornl.service-now.com

Use the ornl.gov Kerberos realm and userid <ornl\kuid>



intidp03 (OSTI)



intidp01 (5600)

Load Balancer



Infrastructure

Set up SPN's for each of the <n> servers in the Ping Fe cluster

By default, Ping Fed will look at the DNS records for ornl.gov to find the IP addresses for the Kerberos systems, which are the domain controllers. A Service Principal Name (SPN) must be configured on the domain controllers for each of the servers in the Ping Fed cluster, specifying the ornl.gov domain account that will be used to exchange the shared secret.

Workstations

Regular Kerberos Refresh (1)

ORNL DMZ

Internet



ornl.service-now.com



88/udp



DCs



User Device (browser)

I'm logged in as `ornl\userid`.
Please give me a Kerberos
TGT and a client session key.

Infrastructure

Workstations

Regular Kerberos Refresh (1)

ORNL DMZ

Internet

The Key Distribution Center (KDC) uses a symmetric encryption key derived from the password for ornl\userID to encrypt the session key. The TGT is encrypted using a key that only the DCs know. The client has to have the user's password to decrypt the client session key, which is used for further communication with the Kerberos Ticket Granting Service (TGS, also part of the DCs). The (encrypted) TGT includes the client IP, the validity period, and the session key.



ornl.service-now.com



DCs



User Device (browser)

Here's your TGT and a session key. They're valid until <time>.

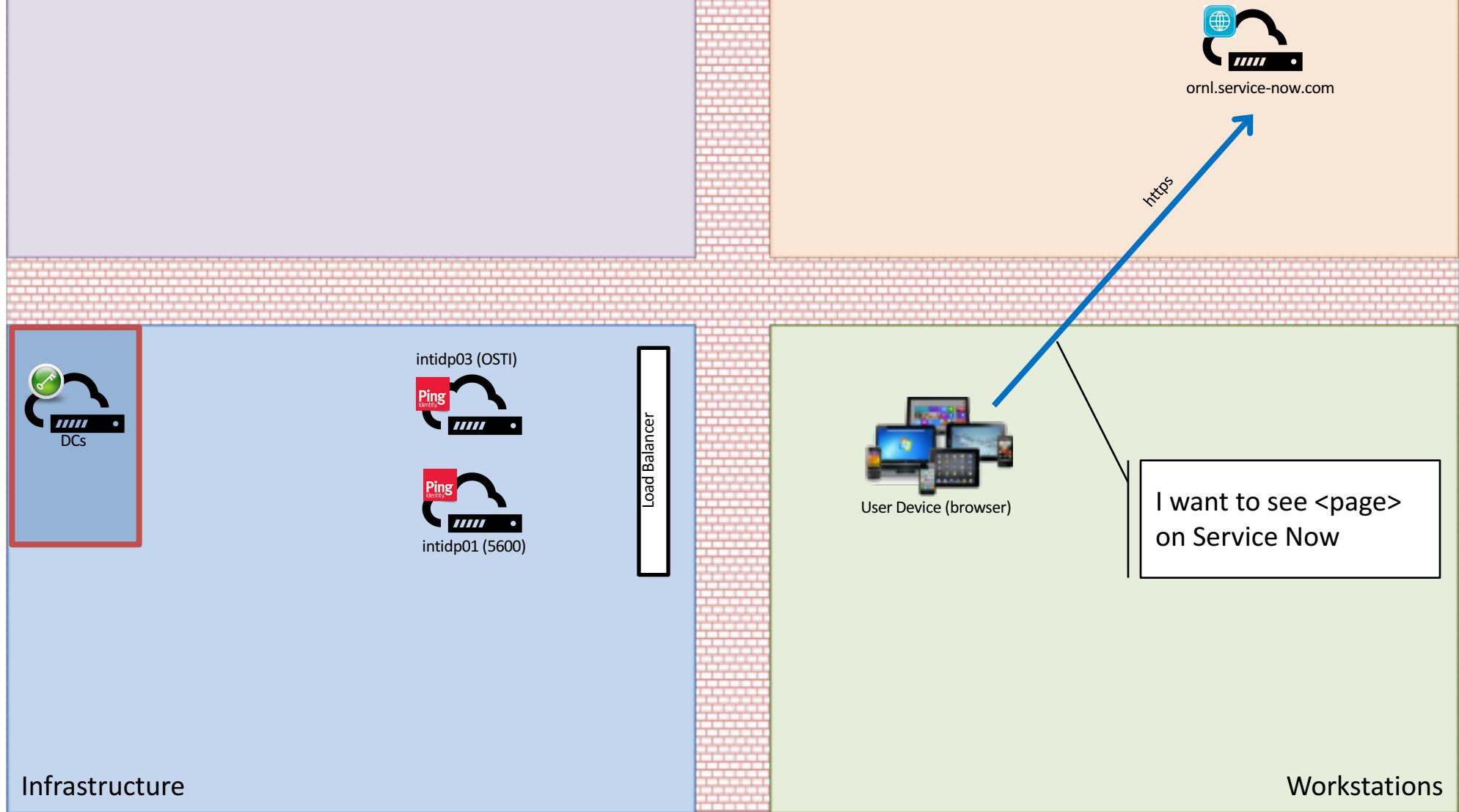
Infrastructure

Workstations

Ping Fed and Service Now: Request Service Now

ORNL DMZ

Internet



Ping Fed and Service Now: Check for existing session

ORNL DMZ

Internet

Does this browser have a current valid Service Now Session Cookie?

Yes – Send requested page and [Use Service Now](#)

No – [Send SAML Request \(internal\)](#)



intidp03 (OSTI)



Ping Identity

intidp01 (5600)

Load Balancer



User Device (browser)

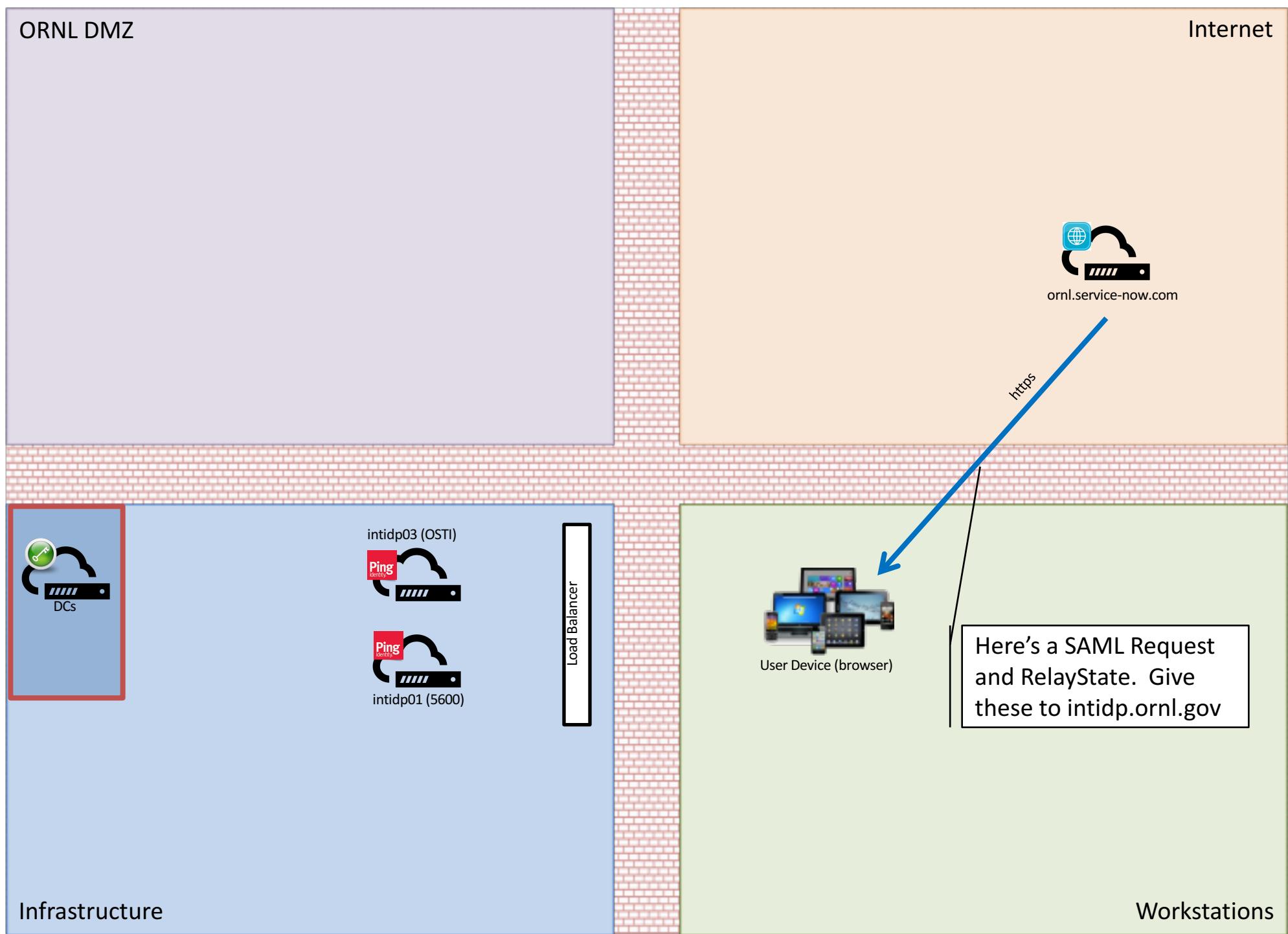
Infrastructure

Workstations

Ping Fed and Service Now: Send SAML Request

ORNL DMZ

Internet



Ping Fed and Service Now: Send SAML Request

ORNL DMZ

Internet



ornl.service-now.com



intidp03 (OSTI)



intidp01 (5600)

https

Load Balancer

https



User Device (browser)

Here's a SAML Request and
RelayState from S-N. I want
to log in and use these.

Infrastructure

Workstations

Ping Fed and Service Now: Check Kerberos

ORNL DMZ

Internet



ornl.service-now.com



intidp03 (OSTI)



intidp01 (5600)

https

Load Balancer

https



User Device (browser)

Do you have an ornl.gov
Kerberos ticket?

Infrastructure

Workstations

Ping Fed and Service Now: Client Check for Kerberos TGT

ORNL DMZ

Internet



ornl.service-now.com



intidp03 (OSTI)



User Device (browser)



intidp01 (5600)

Load Balancer

Infrastructure

Workstations

Do I have an ornl.gov Kerberos Ticket
Granting Ticket?

Yes – [Request Kerberos Service Ticket](#)
No – [Kerberos Response](#)

Ping Fed and Service Now: Request Kerberos Service Ticket

ORNL DMZ

Internet

The client uses the Client Session Key to encrypt the request to the Kerberos Ticket Granting Service (TGS) and sends along the TGT (which is an opaque blob as far as the client is concerned)



ornl.service-now.com



88/udp



User Device (browser)

Here's my TGT. I need a Service Ticket for userid to use intidp.ornl.gov.

Infrastructure

Workstations

Ping Fed and Service Now: Grant Kerberos Service Ticket

ORNL DMZ

Internet

The TGS attempts to decrypt the message with the client session key. If that works, it then decrypts the TGT to see if it's for the requested user, if the IP address matches, and if the TGT is still valid. If all of that works, the TGS uses the server session key to encrypt a Service Ticket for the requested SPN. It then uses the client session key to encrypt the message it sends back to the client.



ornl.service-now.com



88/udp



User Device (browser)

Here's a Service Ticket
for intidp.ornl.gov

Infrastructure

Workstations

Ping Fed and Service Now: Kerberos Response

ORNL DMZ

Internet



Here's a service ticket – [Validate Kerberos Ticket](#)
No, I can't do Kerberos – [Check SSO/Form](#)



ornl.service-now.com



intidp03 (OSTI)



intidp01 (5600)



Load Balancer

https



User Device (browser)

Infrastructure

Workstations

Ping Fed and Service Now: Validate Kerberos Ticket

ORNL DMZ

Internet



ornl.service-now.com



DCs

intidp03 (OSTI)



intidp01 (5600)

Load Balancer



User Device (browser)

Can I decrypt this service ticket with
my server session key? Is the
resulting ticket valid?

Yes – [Get Attributes](#)

No – [Check SSO/Form](#)



Infrastructure

Workstations

Ping Fed and Service Now: Check Form/SSO

ORNL DMZ

Internet



ornl.service-now.com



intidp03 (OSTI)



intidp01 (5600)

Load Balancer



User Device (browser)

Do I already have an HTML Form SSO session for this browser? If yes, go to [Get Attributes](#). If no, go to [Ask for Credentials](#)

Infrastructure

Workstations

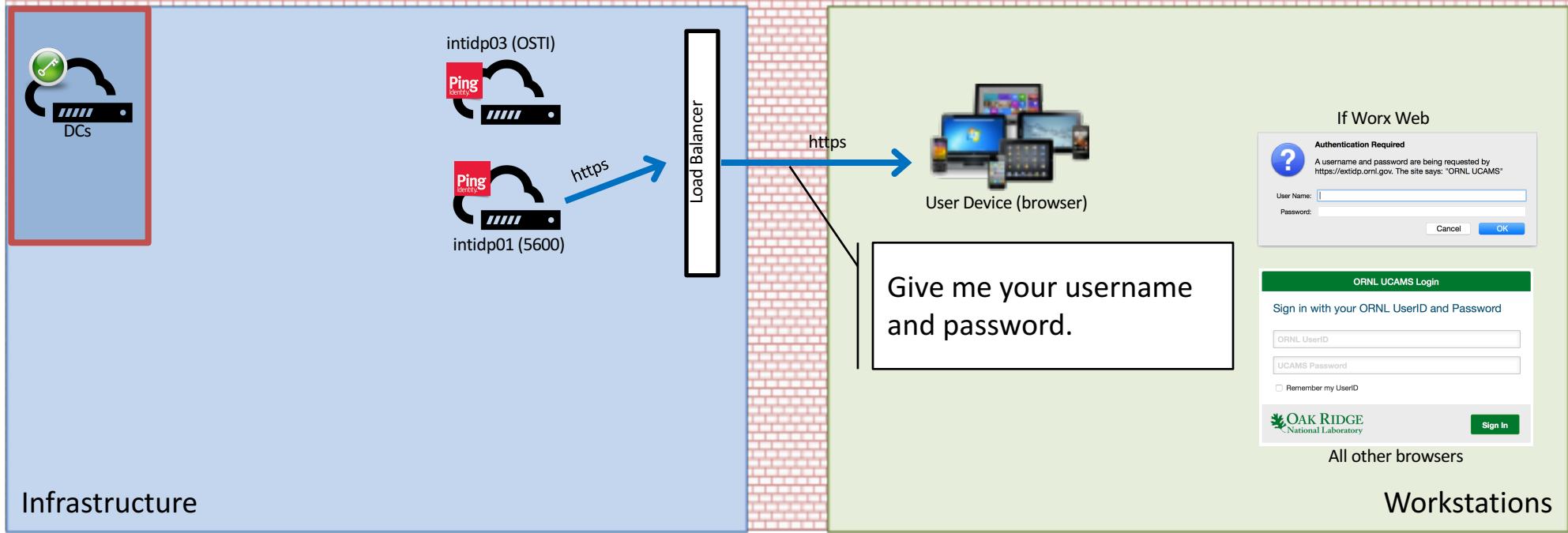
Ping Fed and Service Now: Ask for Credentials

ORNL DMZ

Internet



ornl.service-now.com



Infrastructure

Workstations

Ping Fed and Service Now: Ask for Credentials (2)

ORNL DMZ

Internet



intidp03 (OSTI)
 Ping Identity

intidp01 (5600)
 Ping Identity

https

Load Balancer

https



Here's my username and
password

Infrastructure

Workstations

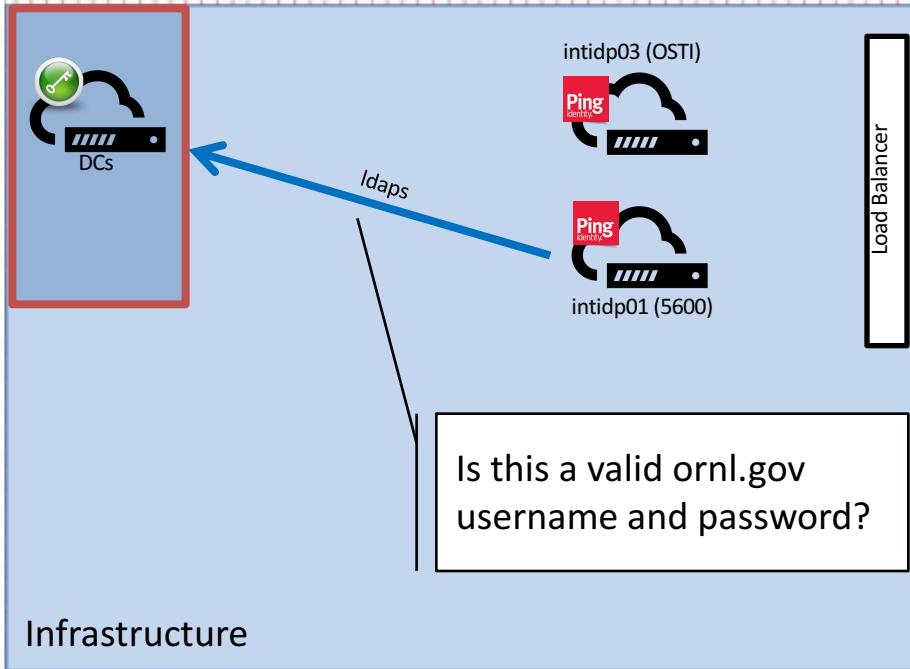
Ping Fed and Service Now: Validate UCAMS Credentials

ORNL DMZ

Internet



ornl.service-now.com



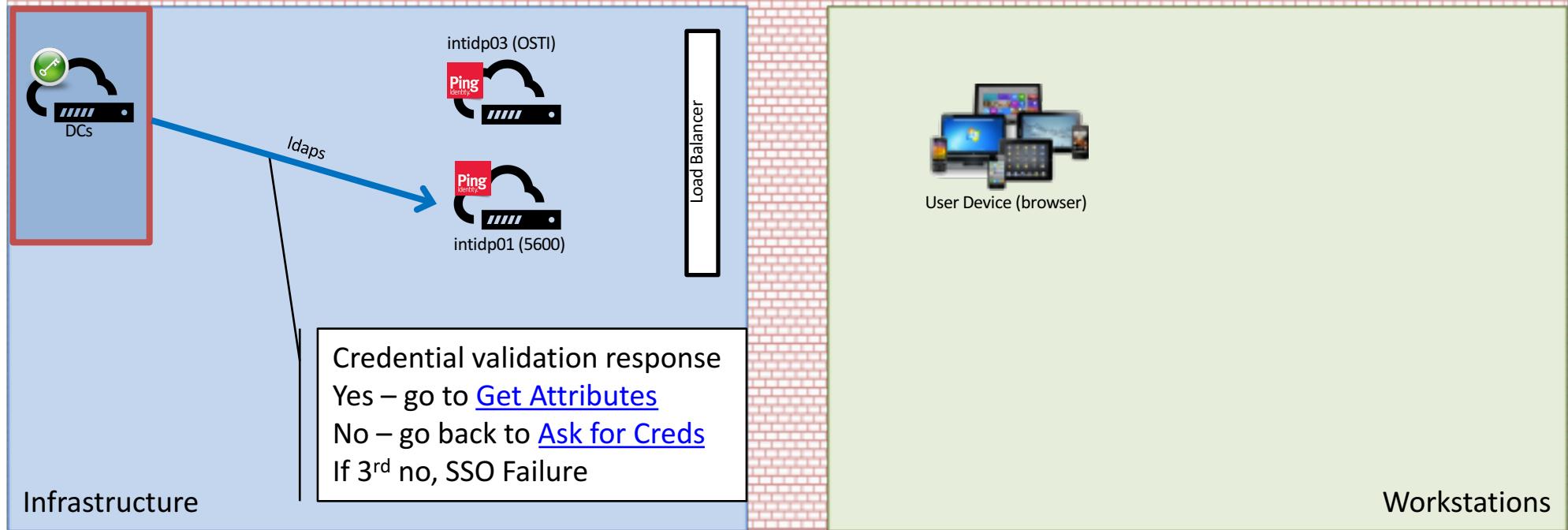
Infrastructure

Workstations

Ping Fed and Service Now: Validate UCAMS Credentials (2)

ORNL DMZ

Internet



Infrastructure

Workstations

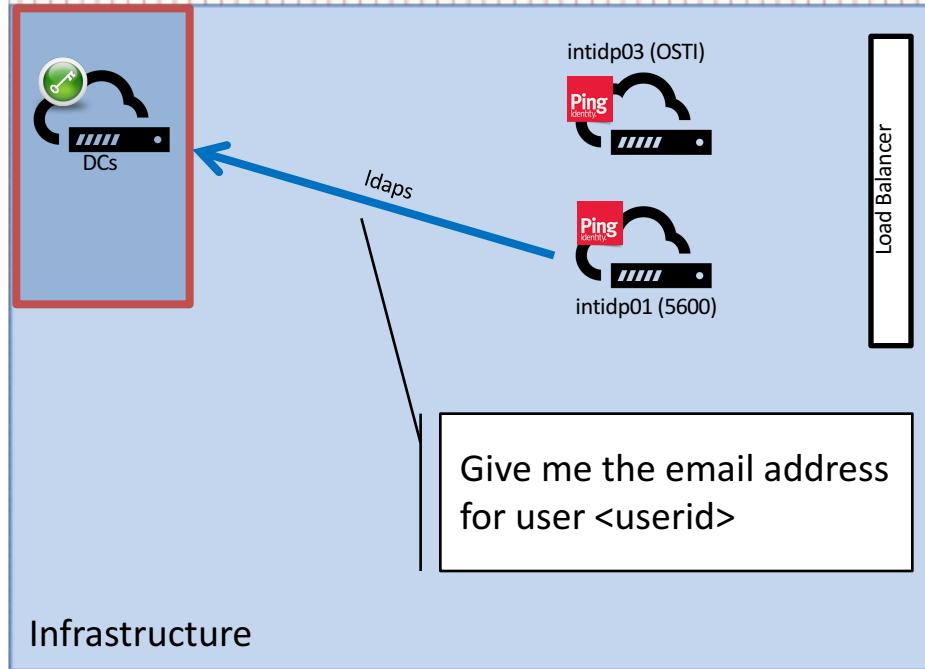
Ping Fed and Service Now: Get Attributes

ORNL DMZ

Internet



ornl.service-now.com



Infrastructure

Internet

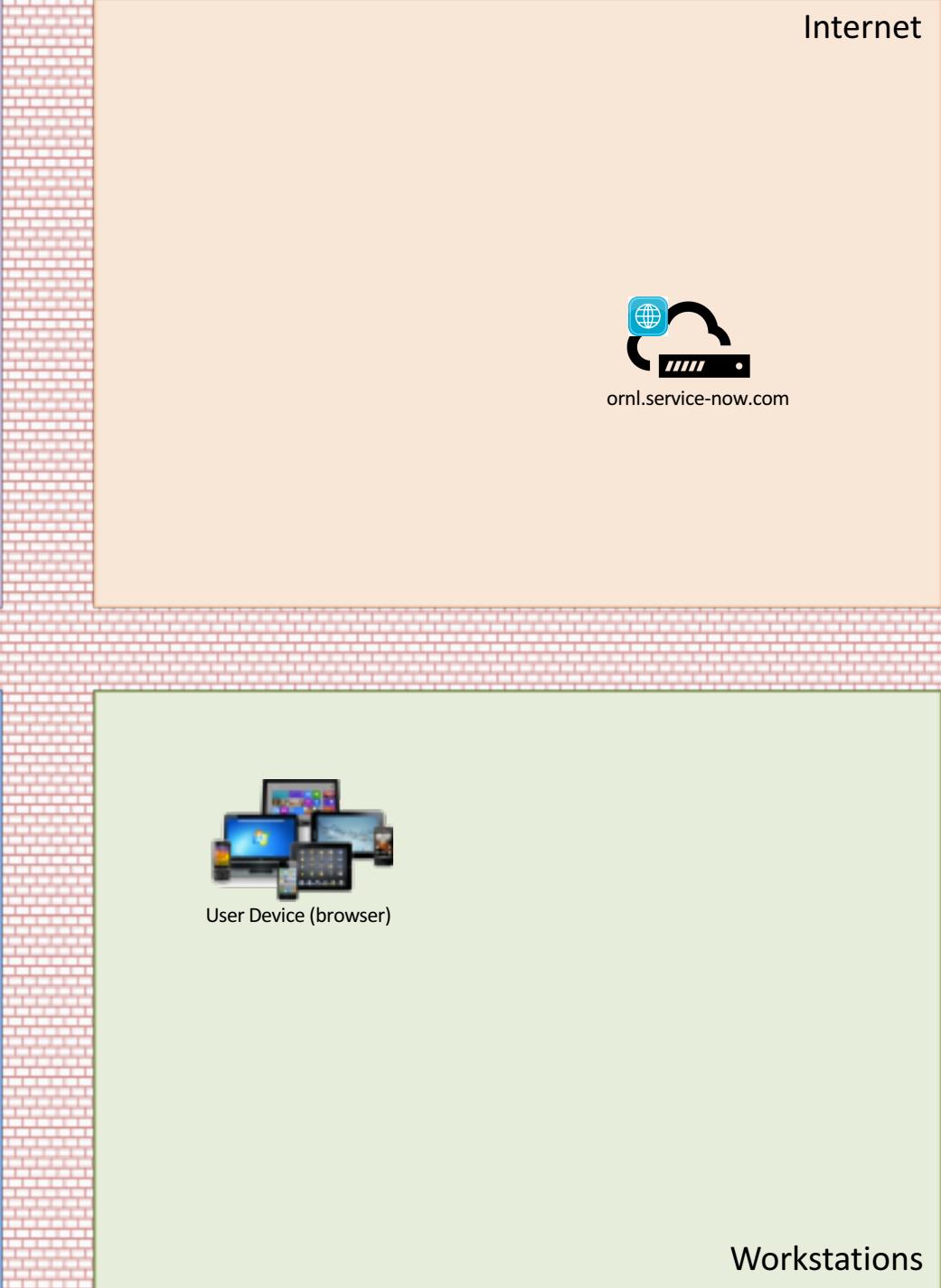
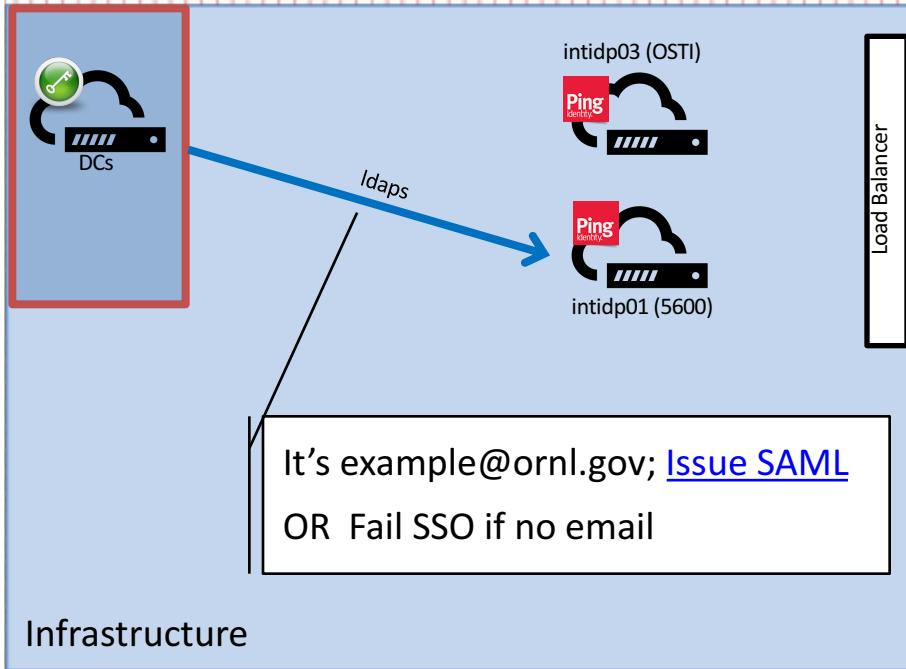
Ping Fed and Service Now: Get Attributes (2)

ORNL DMZ

Internet



ornl.service-now.com



Ping Fed and Service Now: Issue SAML

ORNL DMZ

Internet



ornl.service-now.com



intidp03 (OSTI)



intidp01 (5600)

Load Balancer



User Device (browser)

Infrastructure

Look up the SAML Request identifier and RelayState for this request

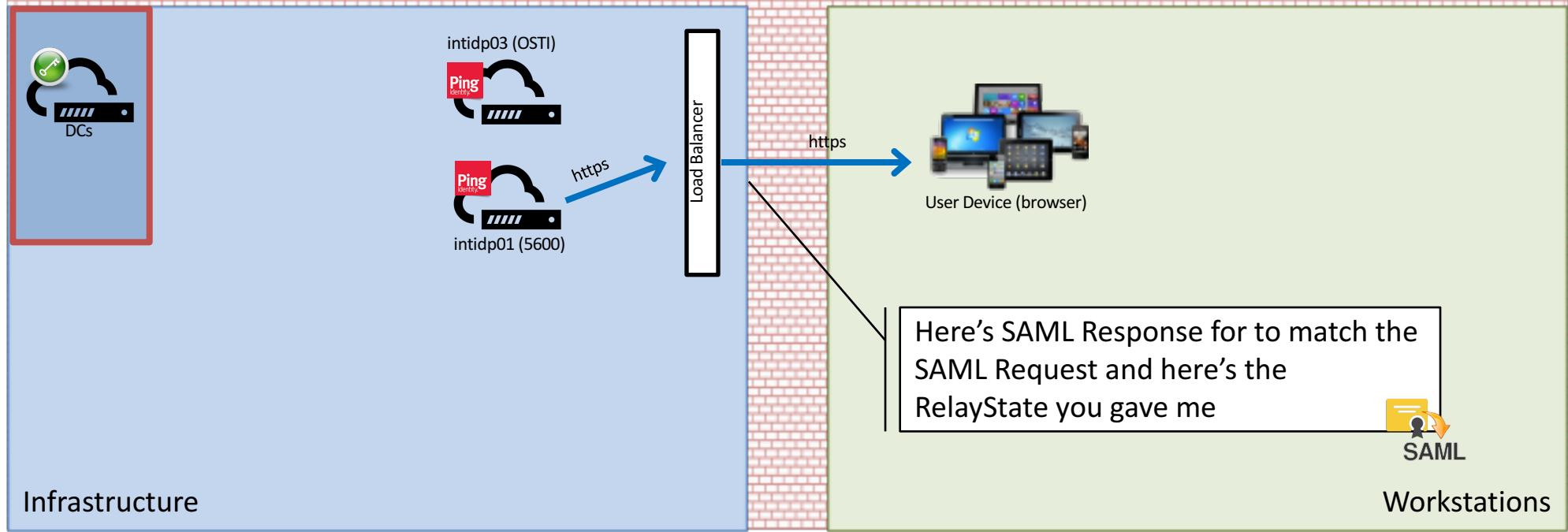


Workstations

Ping Fed and Service Now: Issue SAML (2)

ORNL DMZ

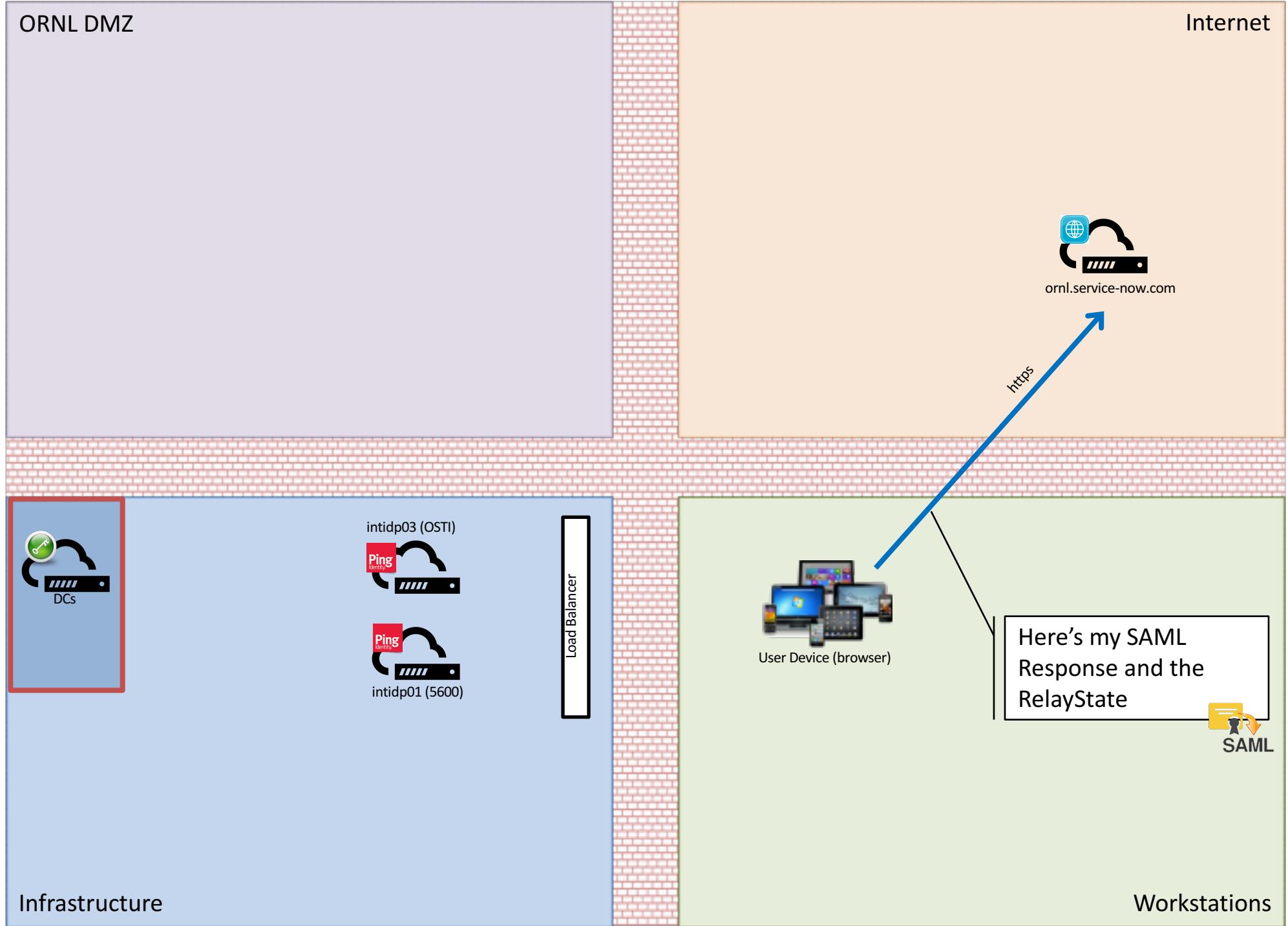
Internet



Ping Fed and Service Now: Exchange SAML

ORNL DMZ

Internet



Ping Fed and Service Now: Exchange SAML (2)

ORNL DMZ

Internet

Is this SAML ticket valid, is it signed with the right private key, if it references a SAML Request is that one I issued, and is example@ornl.gov a valid user?

Yes – Look up original page request (based on RelayState) and [Issue Session Cookie](#)

No – Fail and display logout page



intidp03 (OSTI)



intidp01 (5600)

Load Balancer



User Device (browser)

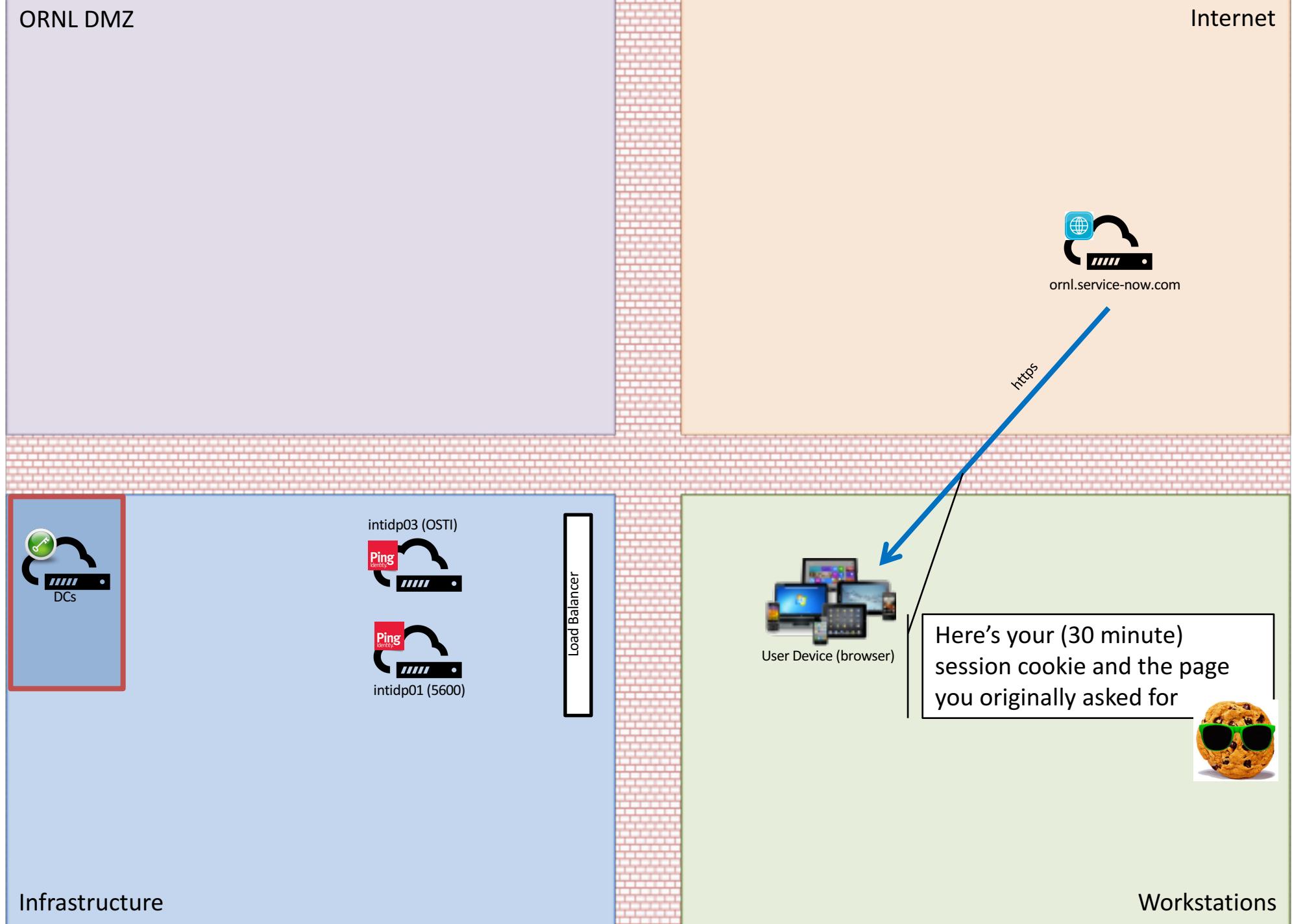
Infrastructure

Workstations

Ping Fed and Service Now: Issue Session Cookie

ORNL DMZ

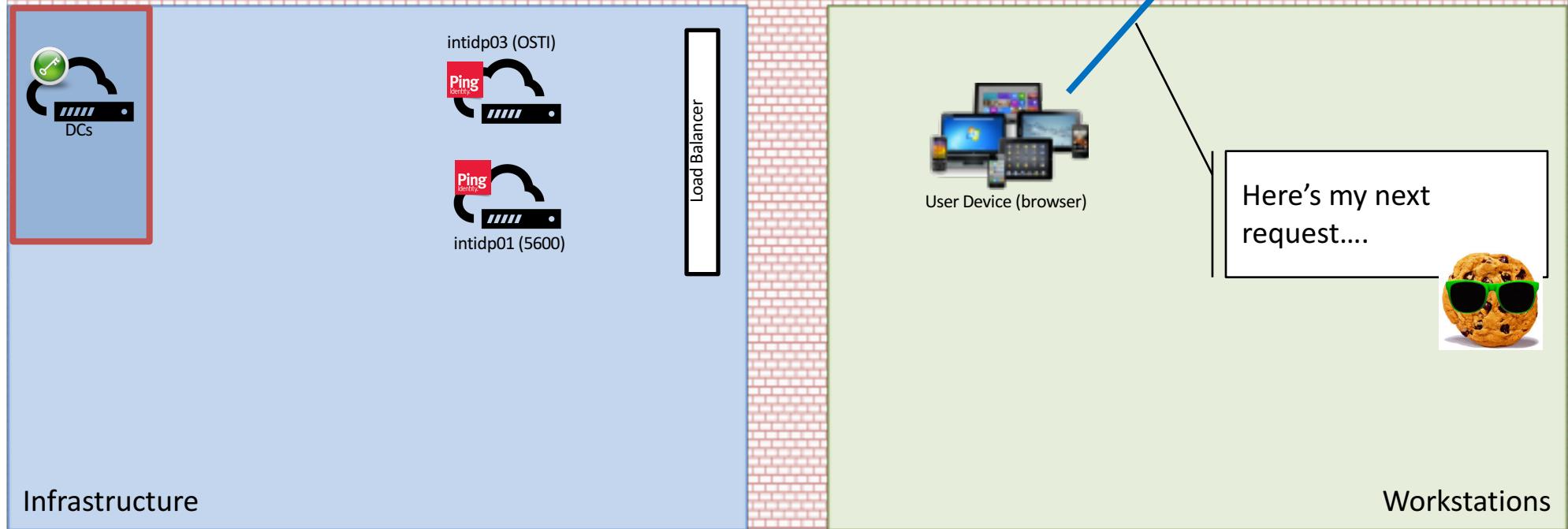
Internet



Ping Fed and Service Now: Use Service Now

ORNL DMZ

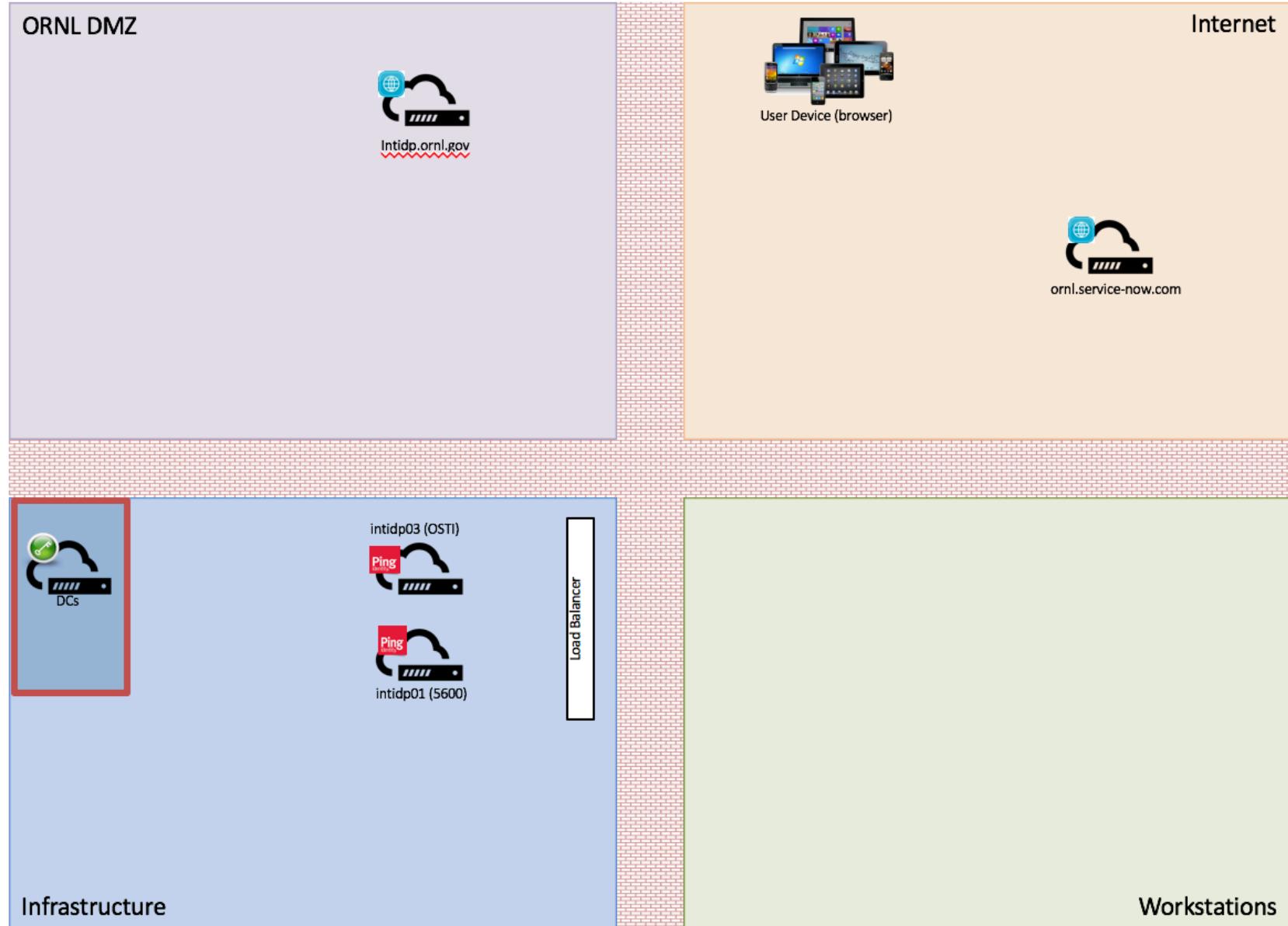
Internet



Infrastructure

Workstations

What happens for Internet user?



Ping Fed and Service Now : Send SAML Request

ORNL DMZ



User Device (browser)

https



Here's a SAML Request
and RelayState. Give
these to intidp.ornl.gov

Internet



intidp03 (OSTI)



intidp01 (5600)

Load Balancer

Infrastructure

Workstations

Ping Fed and Service Now : Send SAML Request (2)

ORNL DMZ

Internet



https



intidp.ornl.gov is split DNS. The server that responds to this from outside ORNL is a dumb web server that displays the same message for all web page requests....

Here's a SAML Request for



intidp03 (OSTI)



intidp01 (5600)

Load Balancer

Infrastructure

Workstations

Ping Fed and Service Now : No SAML Tickets for Internet

ORNL DMZ

Internet



Intidp.ornl.gov

https



User Device (browser)

Sorry, I can't give a SAML ticket unless you're on the ORNL network



ornl.service-now.com

ORNL internal network access only

Sorry, but the web page or service you are attempting to reach is only available from the ORNL internal network. Please use **ORNLAccess, VPN, Worx Web, or Direct Access** to access this service.

If you think you have reached this message in error, please contact the ORNL Solution Center ([865-241-6765](tel:865-241-6765) or solution@ornl.gov). If you can send the diagnostic information provided below (a screen shot of this page or copy/paste the information into an email), that will help us trace down the issue more quickly.

Diagnostic Information

Service: SAML IdP (Ping Federate)
Sat Jul 30 2016 09:17:59 GMT-0400 (EDT)
SP Id: Not found



Security Notice

Infrastructure

Workstations

Setting up and Debugging

- SAML Tracer (Firefox Add-in)
- SAML Message Decoder (Chrome)
- IE Message tracing (shift-F12?)
- Logs. Especially into a search/aggregate tool
 - The IdP will get blamed when things break

SAML Enabling an App

- Apache: Easy. Use `mod_auth_mellon`
 - Saves POST when authentication is needed
- Nginx: `auth_request` module
 - Not something I've actually used
- IIS: No good solution. Have to do it in the app itself or use something like OpenToken
- SAML Enable app itself
 - PHP: SimpleSAMLphp (quite robust)

SAML and Federation: 3 patterns

- Where Are You From (WAYF)?
 - Pick your Institution
 - Heavily used with InCommon
- Who Are You?
 - Email address (typically) drives IdP selection
 - Used by Office 365
- Subdomain classing
 - e.g. ornl.service-now.com, ornl.bluejeans.com

Select An Identity Provider:

North Carolina State University
Northern Illinois University
Northwestern University
Oak Ridge National Laboratory

Search:

Remember this selection:

Log On

By selecting "Log On", you agree to [CILogon's privacy policy](#).

Security

- IdP Private Key protection essential
 - Can use a Hardware Storage Module
- Should be over TLS
- Encrypt with SP PubKey if sensitive data
 - User's browser sees everything
- SP can ignore Responses it didn't request
 - IdP Initiated: Unsolicited from SP perspective
 - SP Initiated: SP sends SAML Request to IdP
- Artifact binding: Sends a nonce in Response
 - SP calls authenticated IdP endpoint with nonce to get user identity and attributes

Questions?

