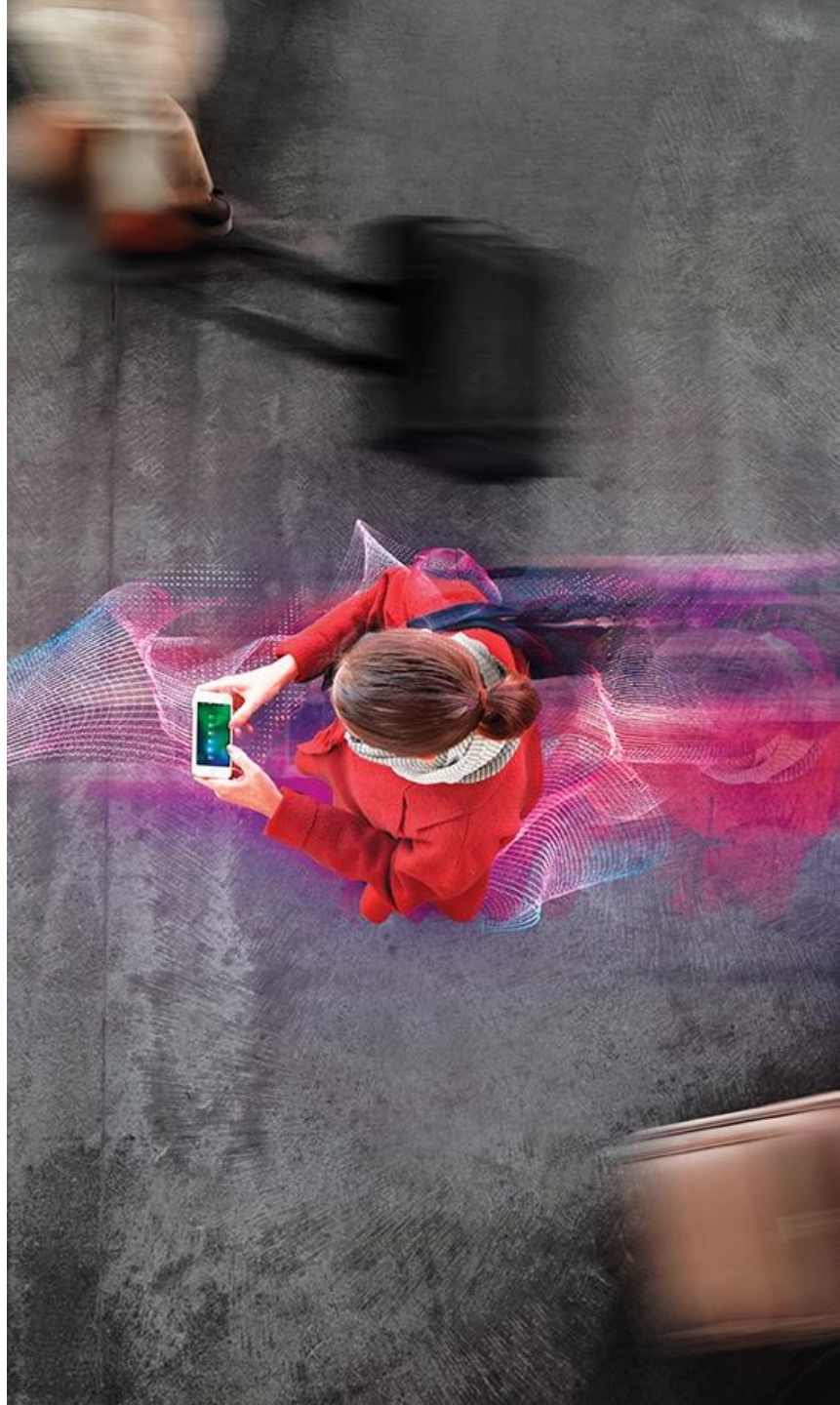
Digicomp Citrix-Day 2015 Networking Update

Zürich, 11.11.2015

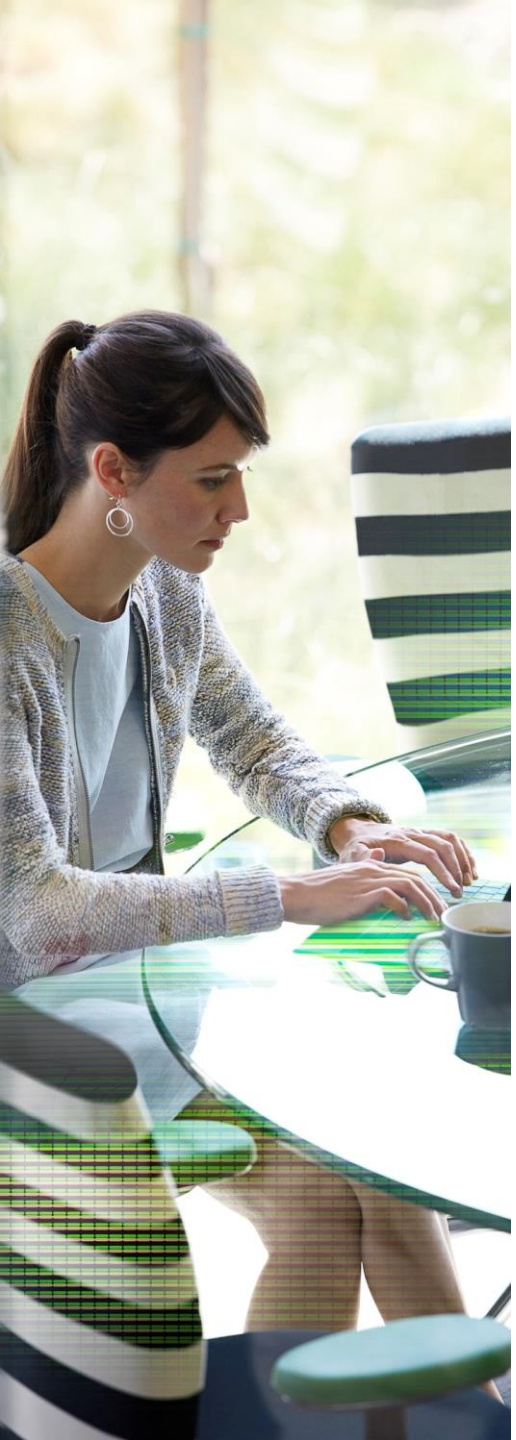
Simeon Bosshard

Citrix Systems International GmbH



Agenda

- NetScaler 11
  - Unified Gateway
  - SDX
  - General Improvements
- CloudBridge
  - WAN Optimization 7.4
  - VirtualWAN – WAN Optimization
  - VirtualWAN / VirtualWAN Center
  - HDX Optimization



NetScaler 11

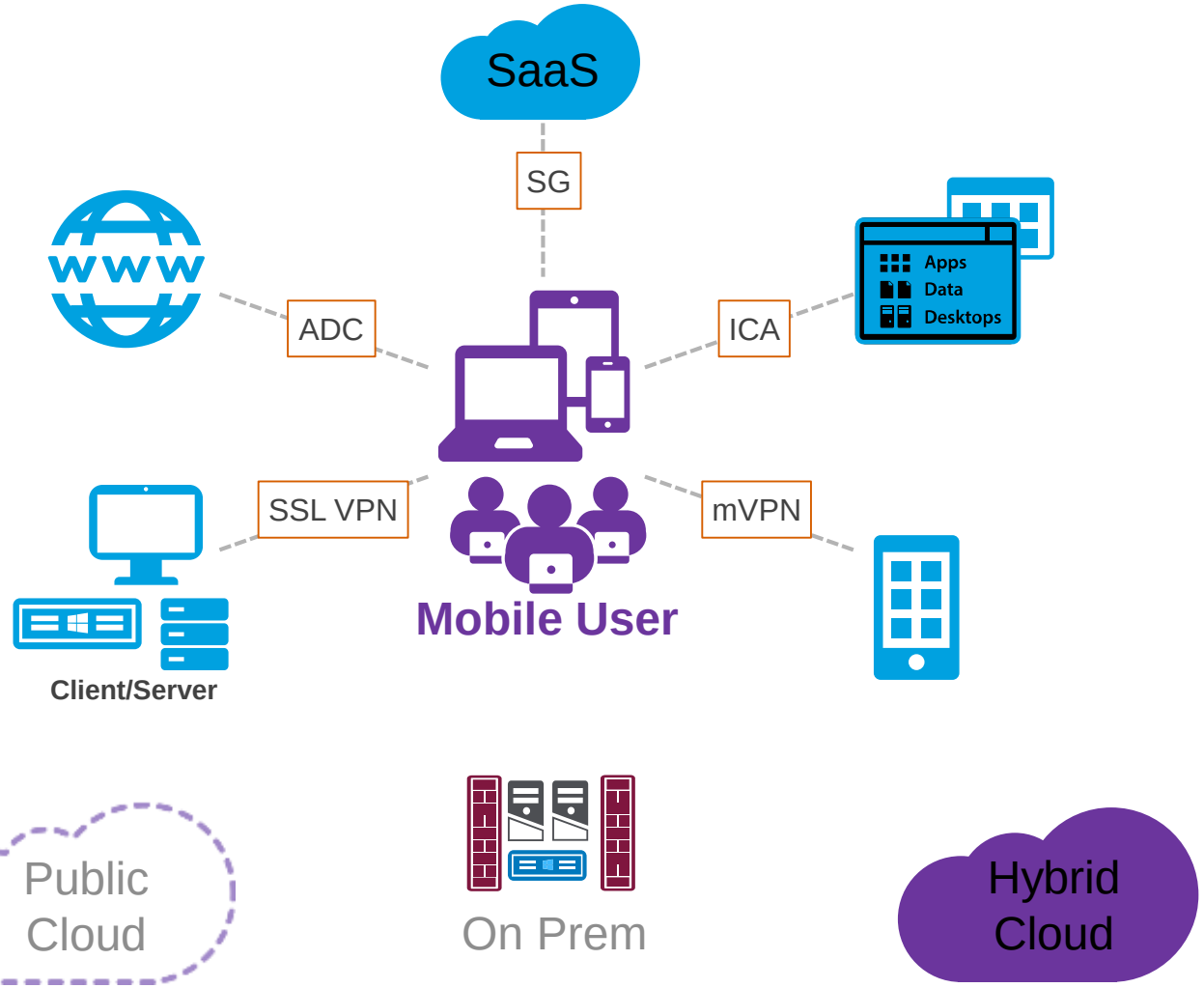
Unified Gateway

Unified Gateway

(Key Use Cases)

- Access Unification
- Smart Access 2.0
- Portal Customization
- CVPN Infrastructure
- Client Plugins

Why Unified Gateway ?

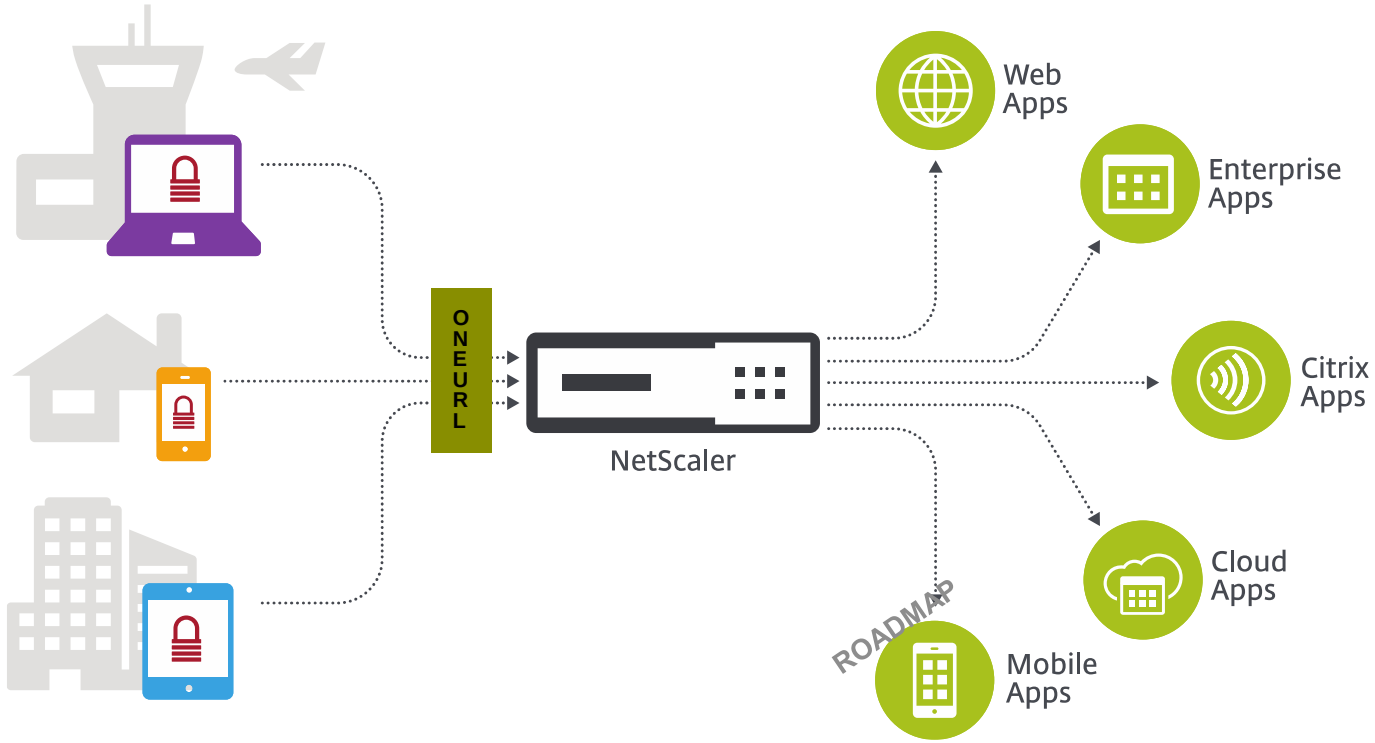


Multiple point solutions result in:

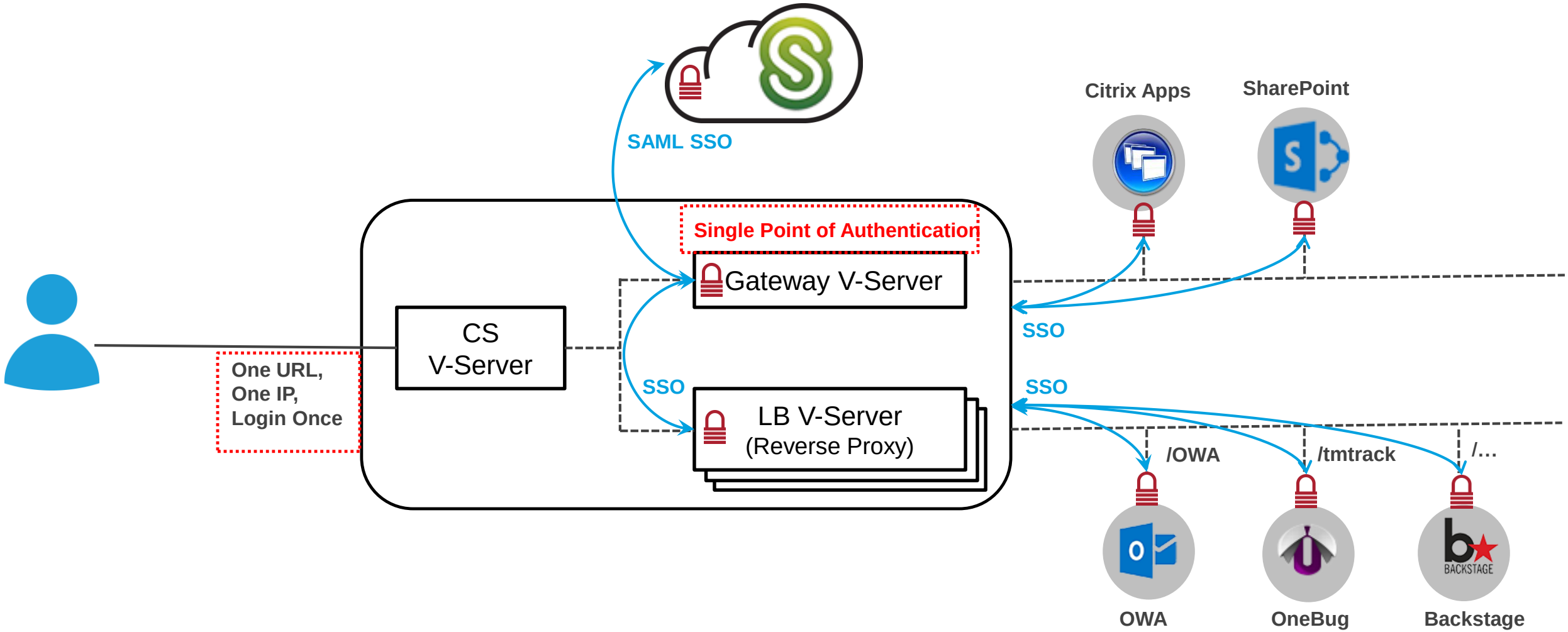
- Multiple URLs, Limited or poor end user experience
- Complicated and hard to manage Infrastructure
- Multiple islands, limited integration between products/solutions
- Misconfiguration of security and access policies
- Re-authentication for all the applications.

Unified Gateway - One URL to any application

- One addressable URL/FQDN
- “Login Once” and achieve seamless SSO to WebApps, Enterprise Apps, Citrix Apps, CloudApps (Mobile Apps is in the works)
- A single pane of glass for Configuration, Security and Control



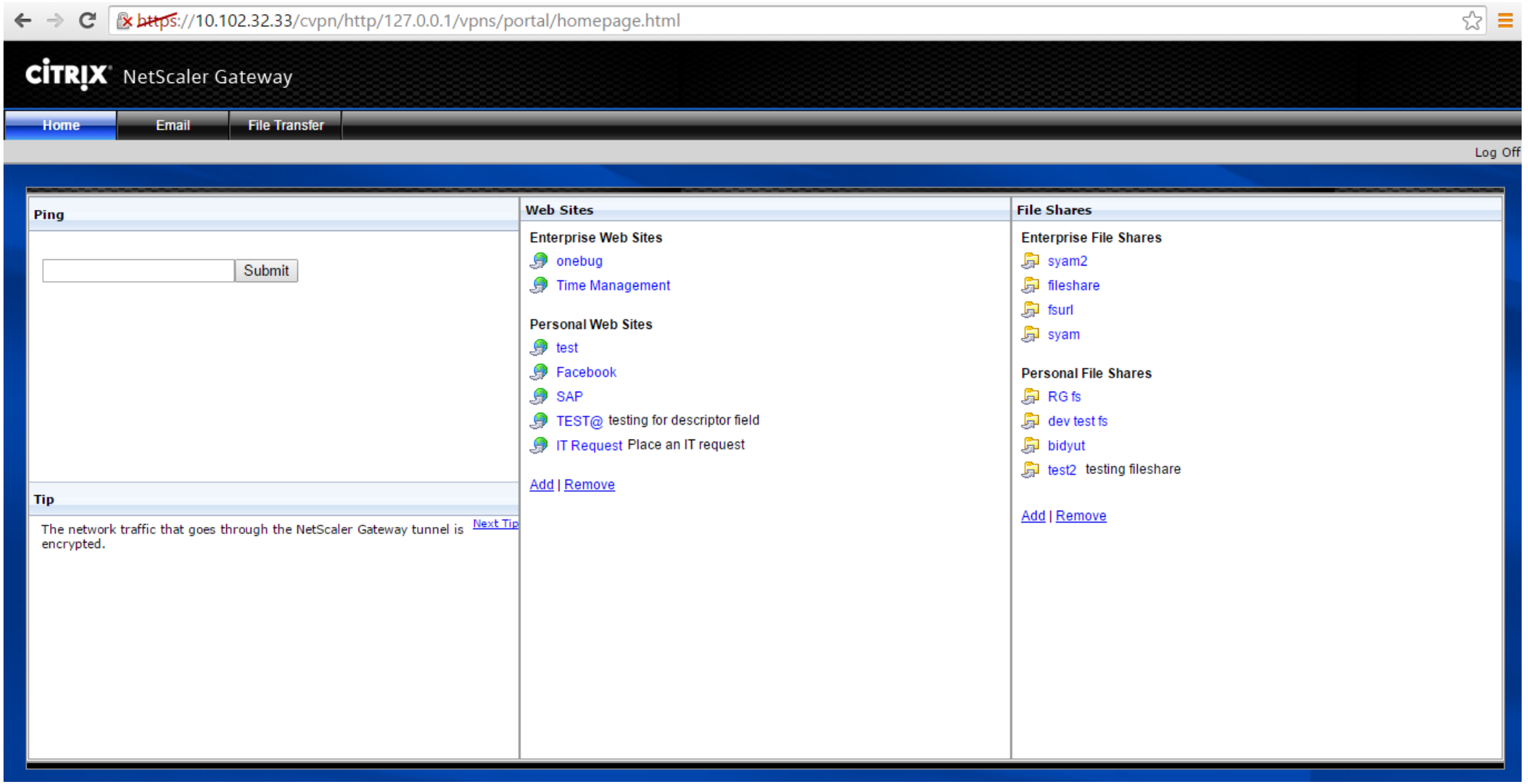
Unified Gateway – Building blocks



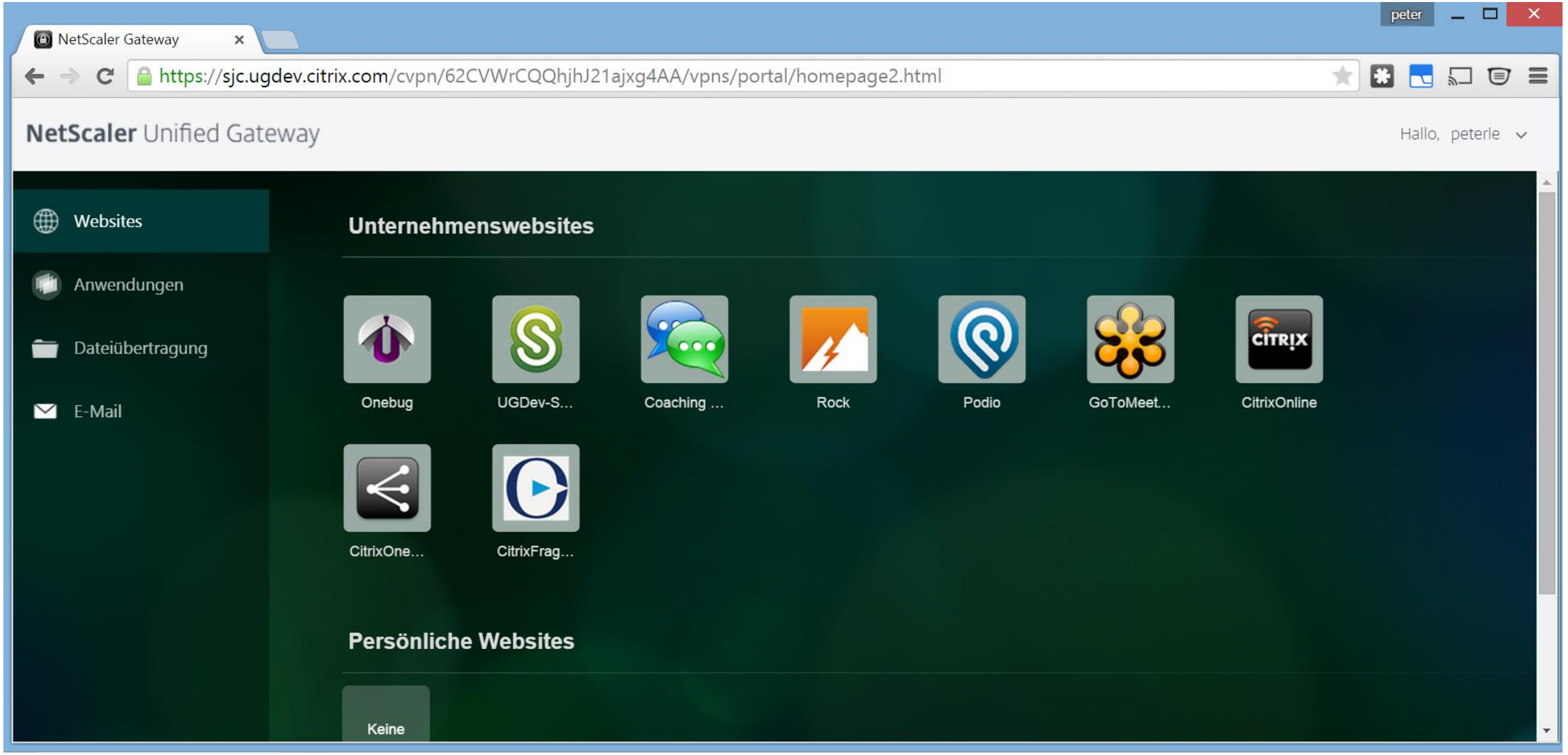
Unified Gateway- What's new in Gateway?

- Gateway vserver
  - can be behind CS vserver.
  - Does not need IP/port.
  - Does not need SSL certs(SSL certs are bound to front end CS vserver)
  - Single point of configuration for all policies(Authentication/authorization/session)
- Login once
  - One login for all GW/TM/SaaS apps that are published on gateway portal.
- Logout once
  - Single logout for all TM web apps/enterprise apps behind Unified Gateway.

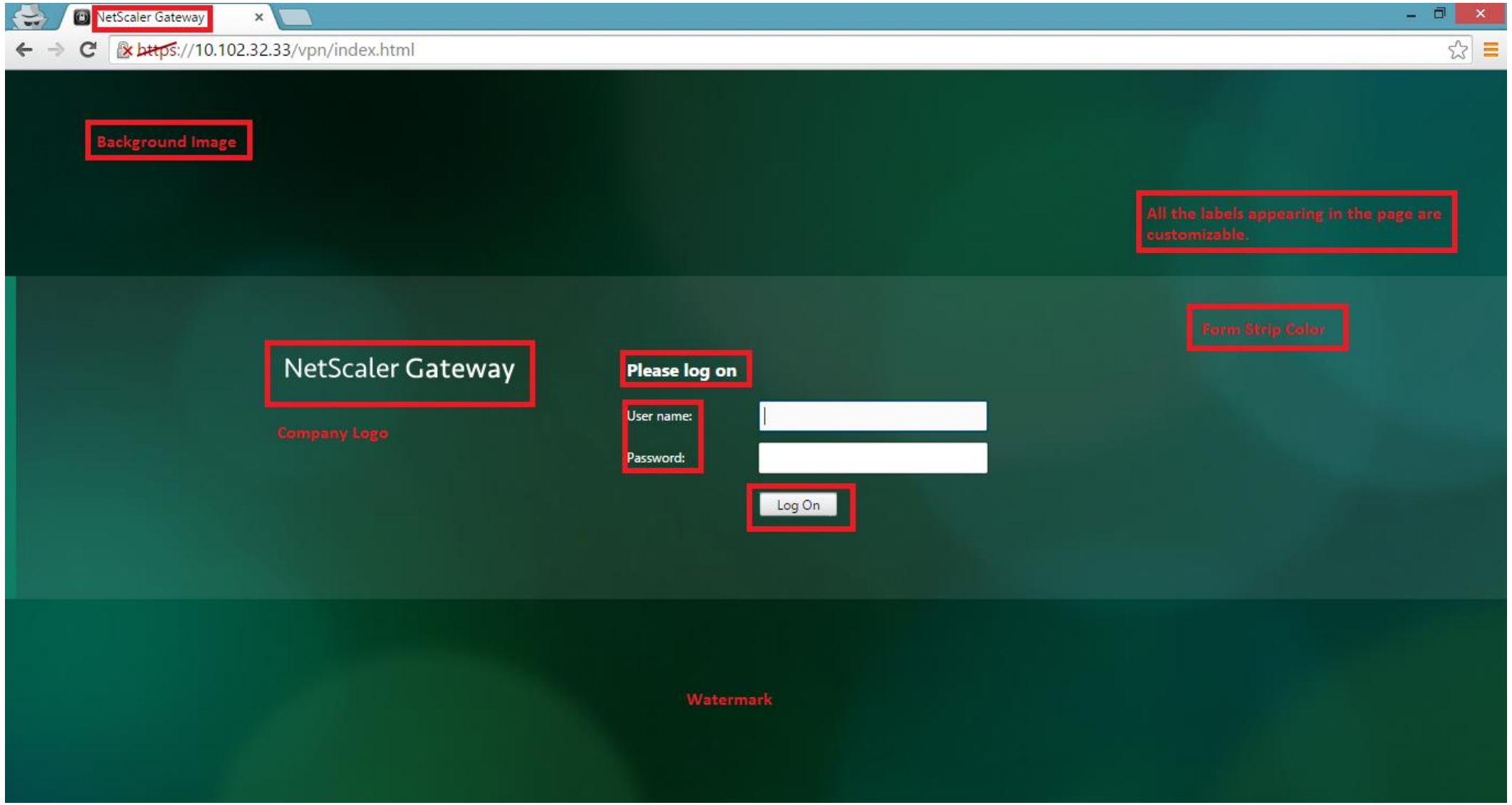
Default theme homepage:



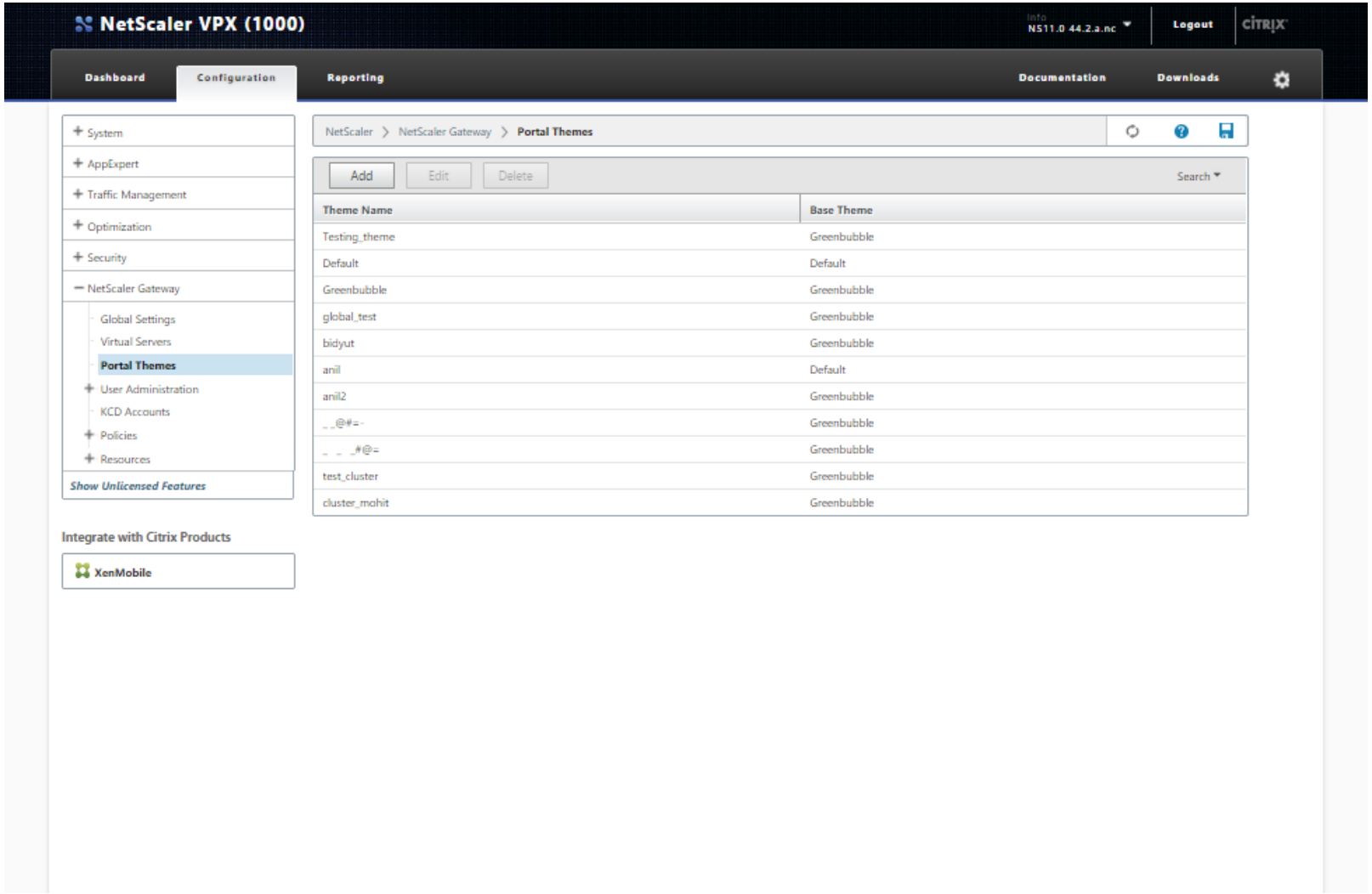
New homepage for Greenbubble theme



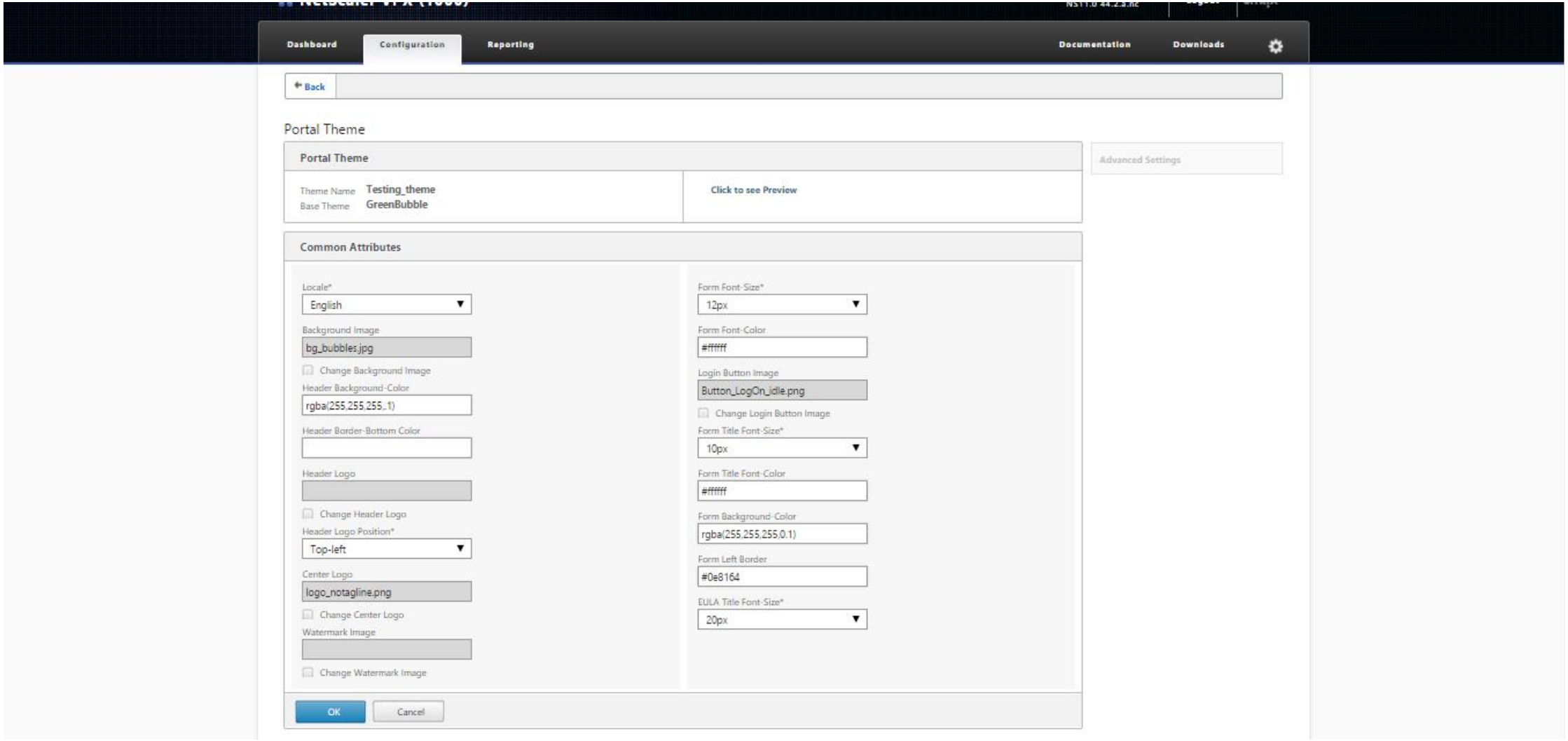
Customization

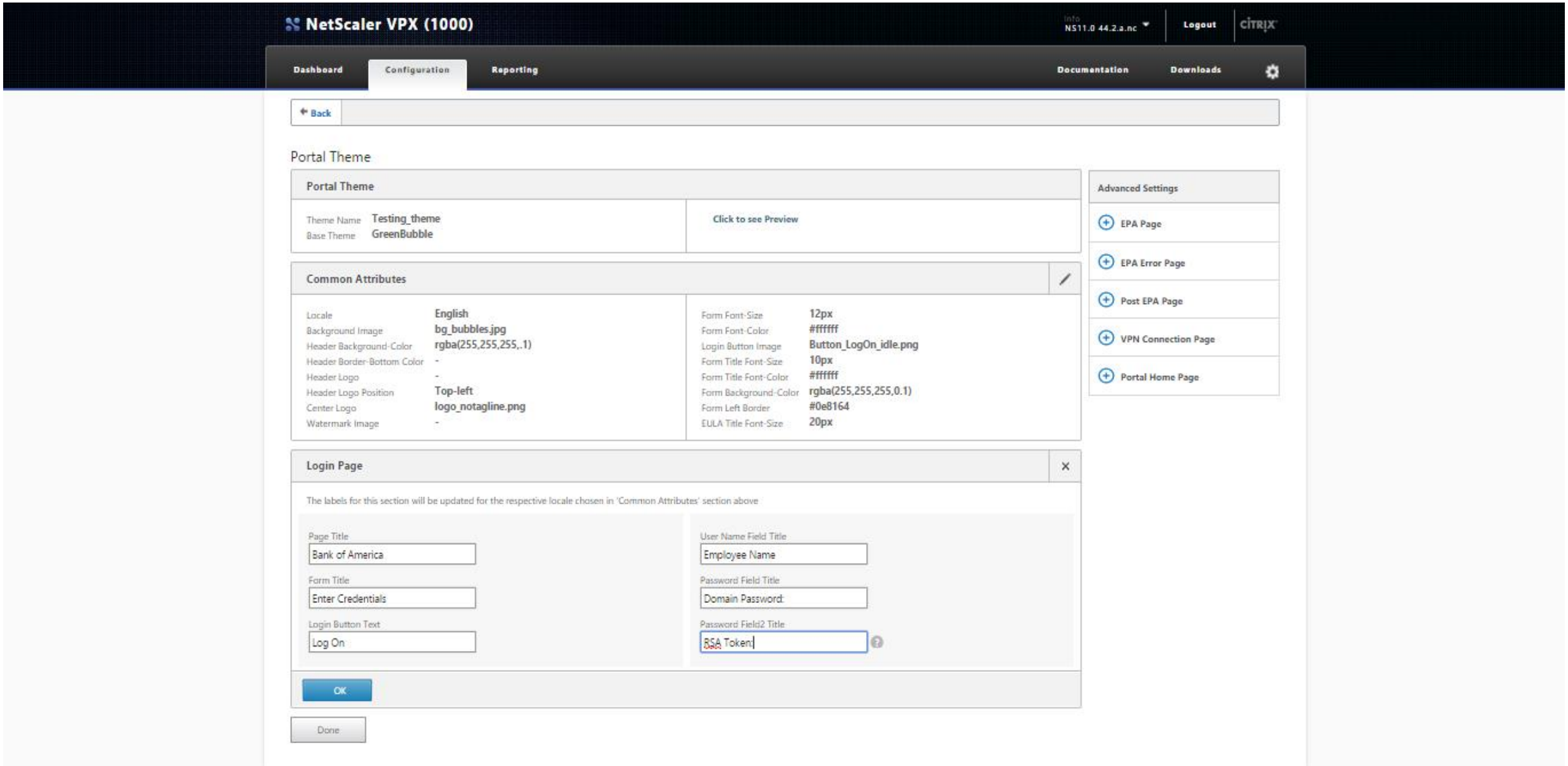


Admin GUI



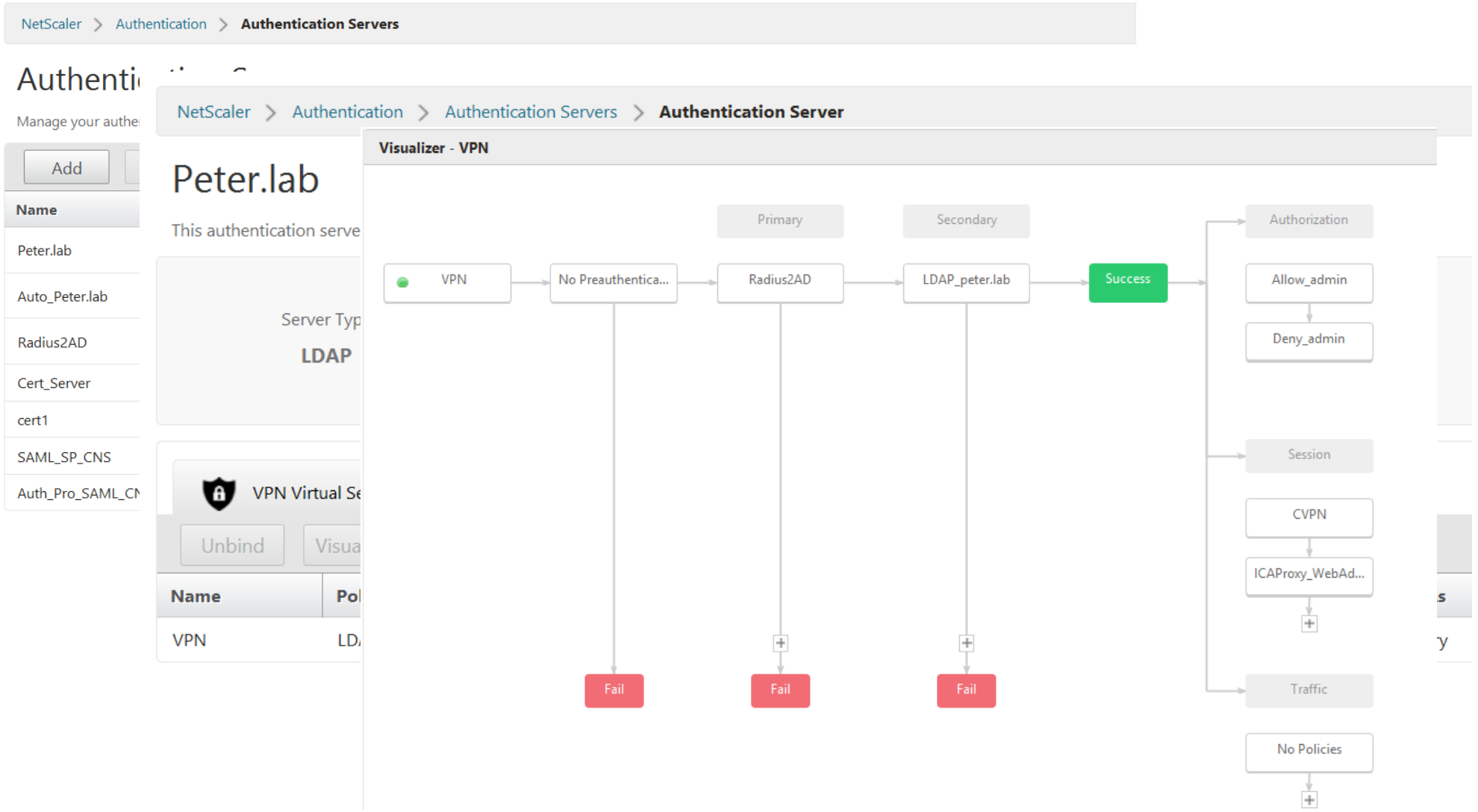
Portal Customization Wizard flow



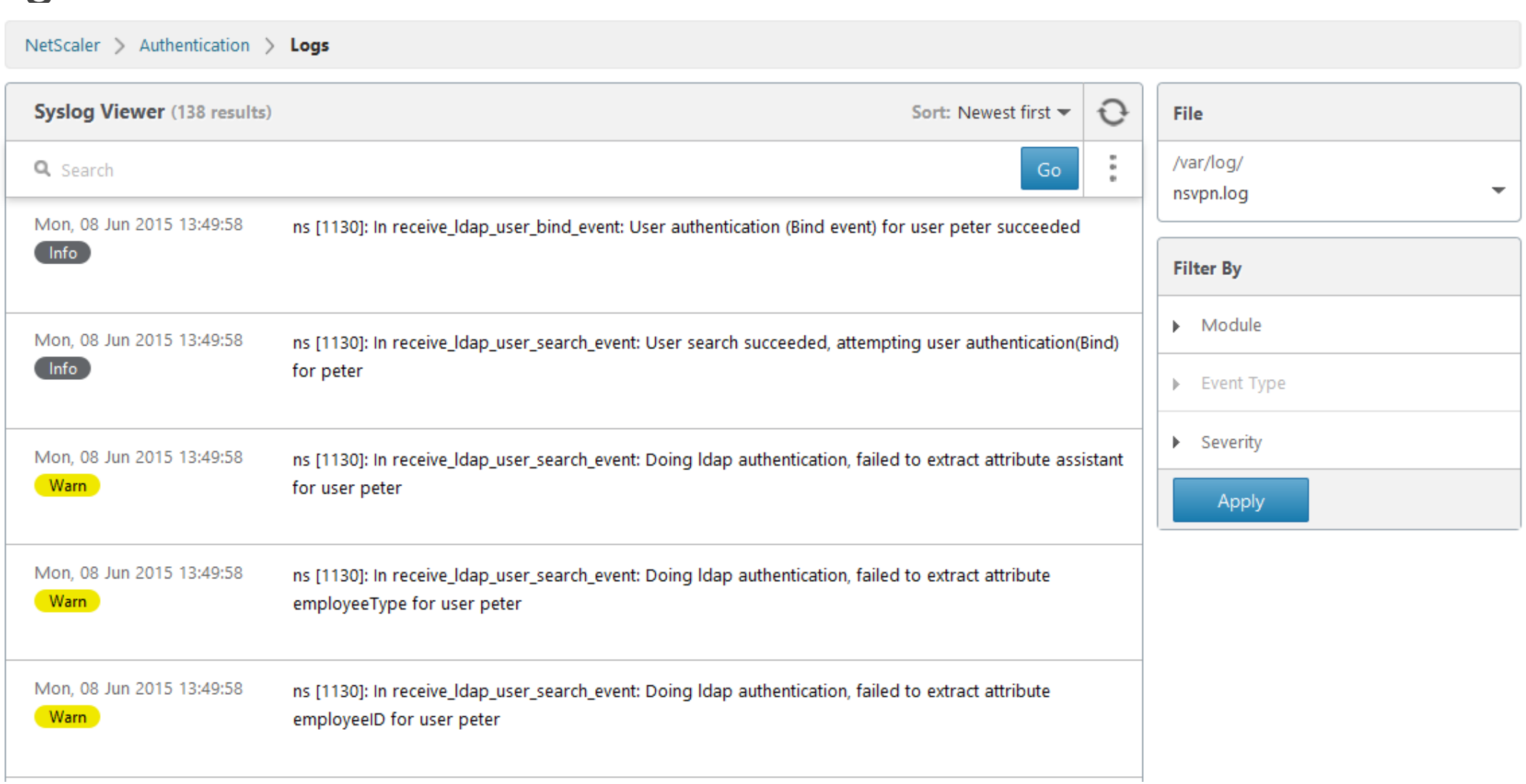


Major customizable parameters. Includes CSS styling which will be consistently applied to all pages. Individual pages labels are also customizable.

Authentication Dashboard

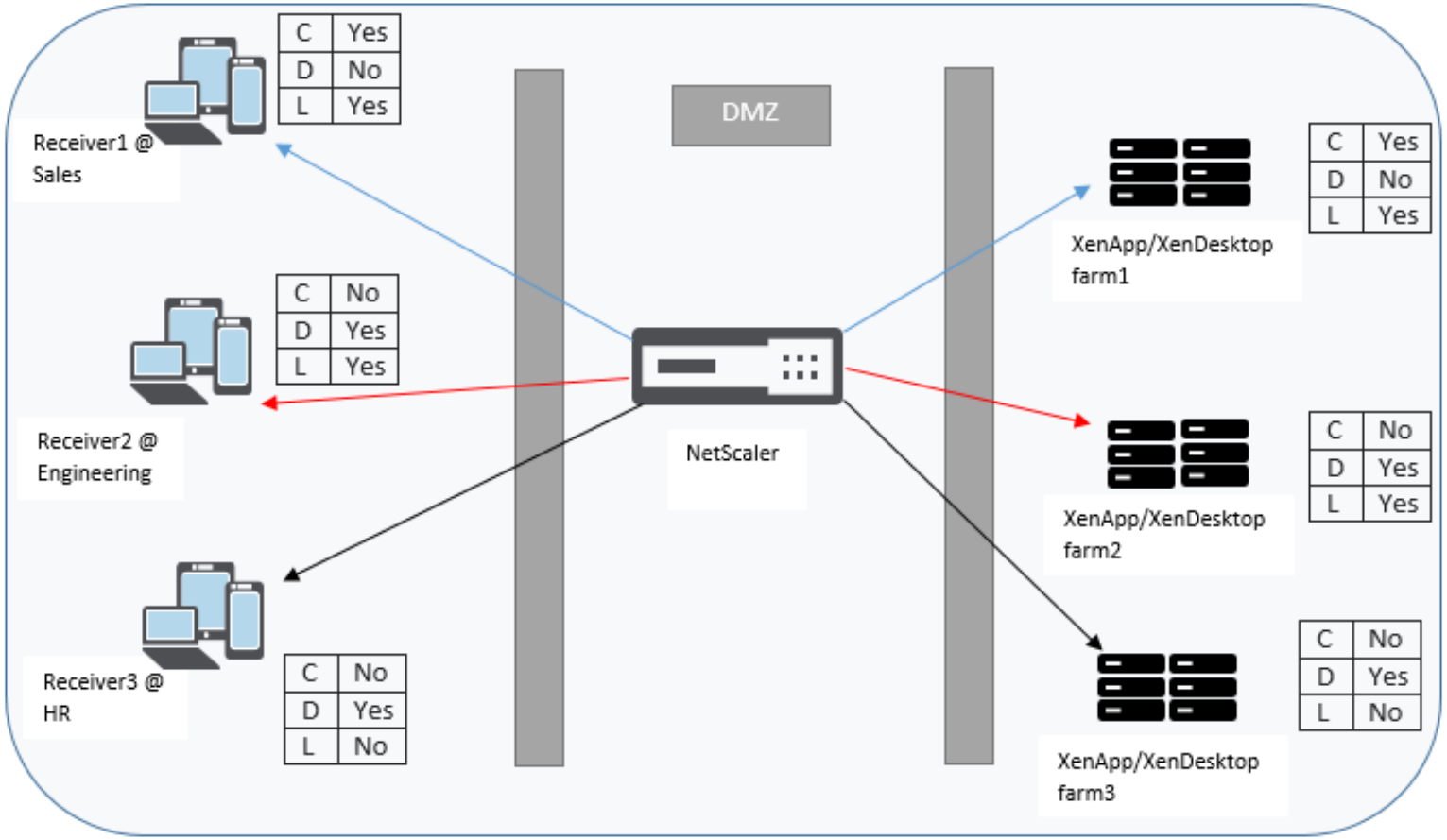


Syslog Viewer



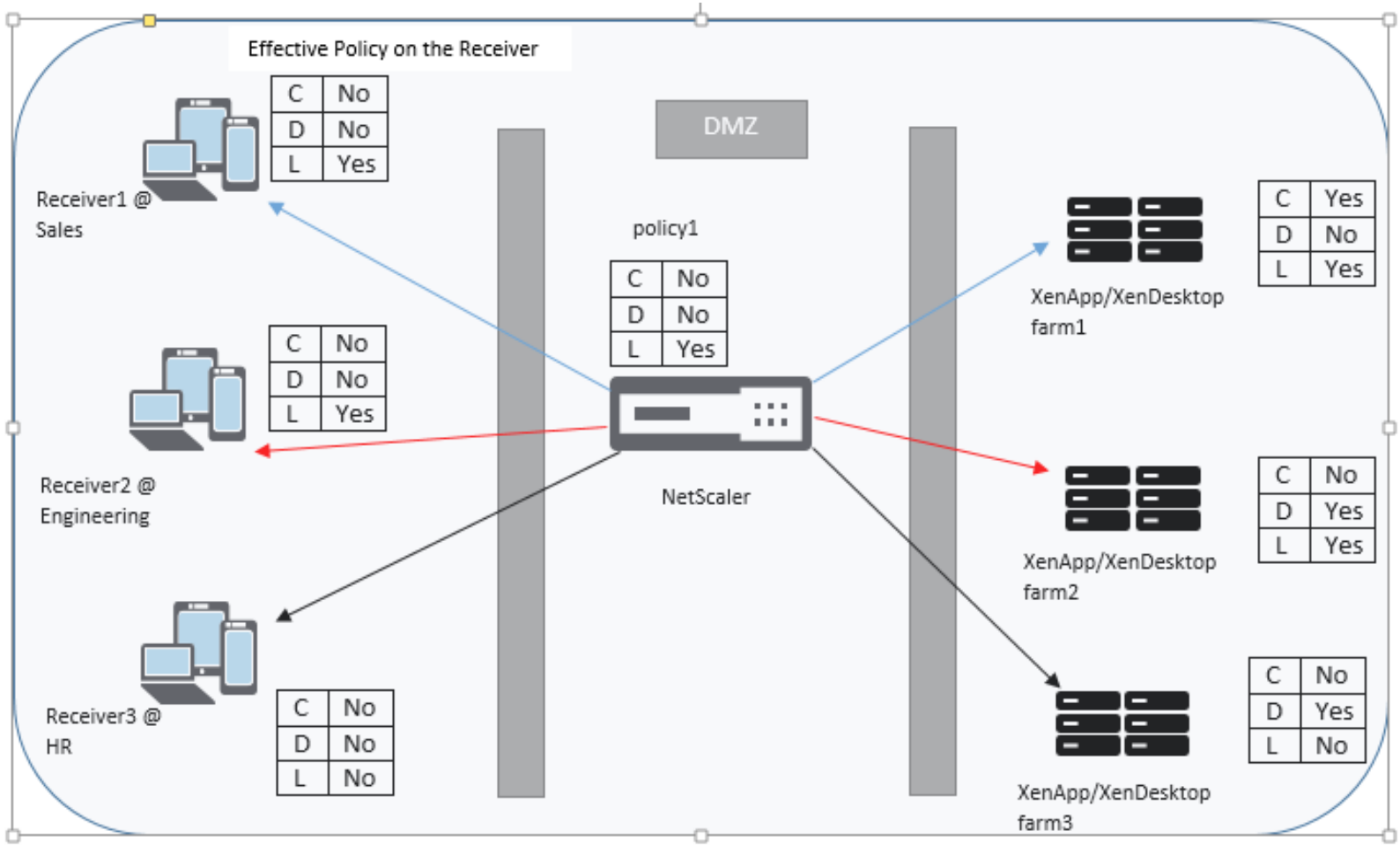
SmartAccess

C,D,L are applications in this example where C = Clipboard access, D = Drive mapping and L = LPT port access.



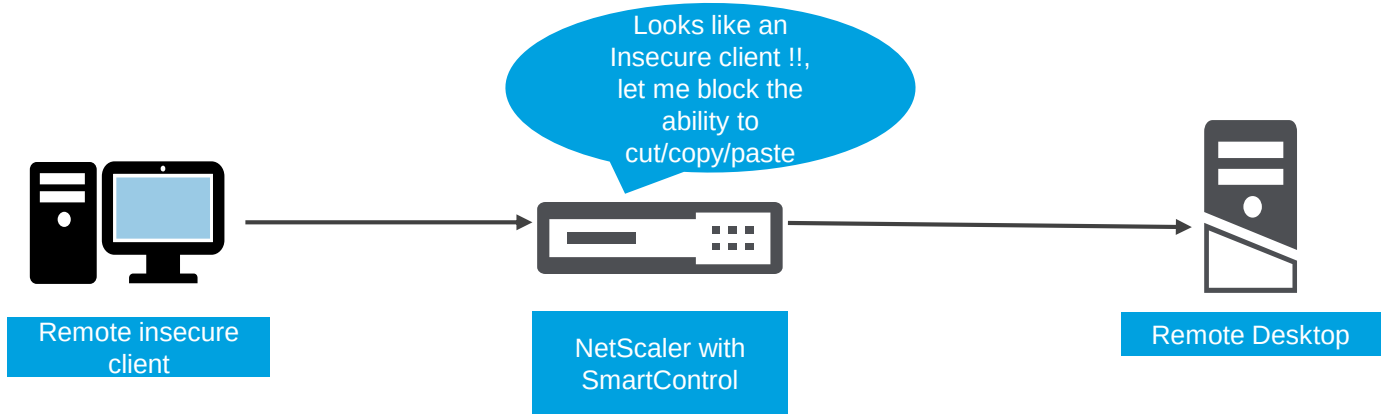
SmartControl

Overriding capability on NetScaler and the effective policy on Receiver.



What is the difference between SmartAccess and SmartControl?

- SmartAccess: access to published application controlled in XA/XD policy engine with the help of session polices results from the NS.
- SmartControl: NetScaler becomes a single point of configuration and enforcement. The NS takes the decision to block access to any features.



SmartControl: What can be controlled?

All of these features can be controlled.

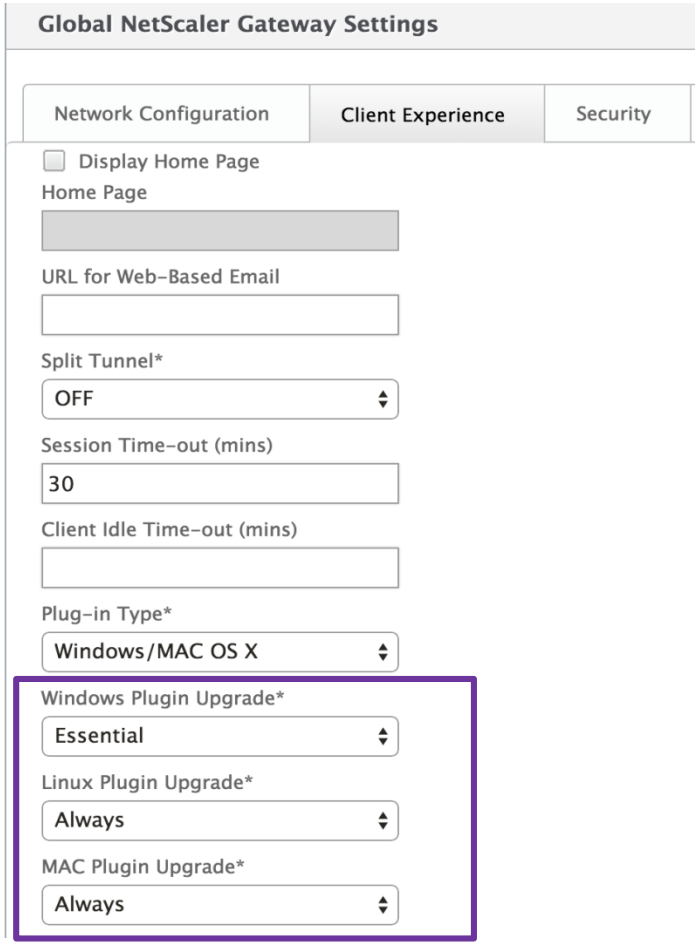
- Client clipboard redirection
- Client Drive mapping
- Client USB Device Redirection
- Client audio redirection
- Client COM port redirection
- Client LPT port redirection
- Client printer redirection
- Multi stream
- File sharing for Receiver for HTML5

SmartControl requires Platinum License!

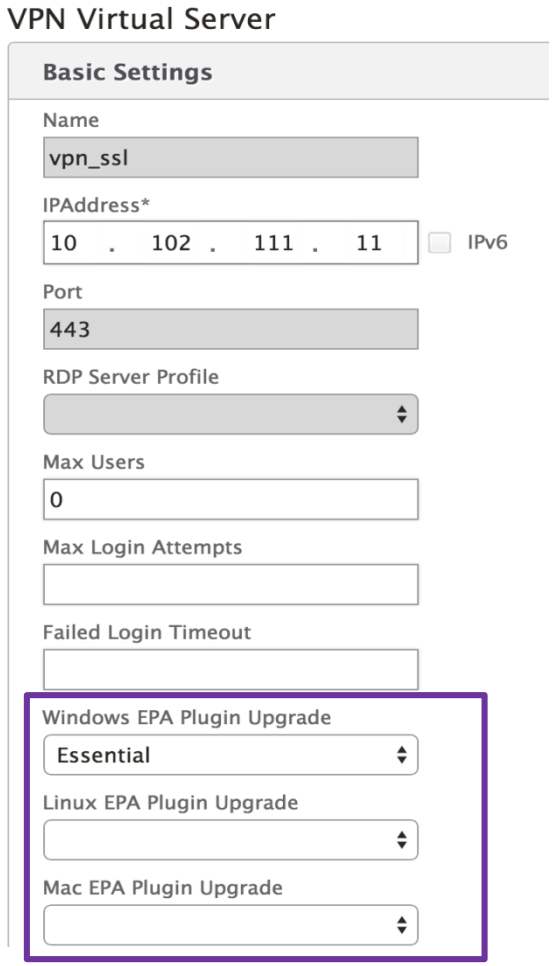
No hiding of published applications!

- Rather than making the admin configure capabilities on multiple backend XA/XD servers, with SmartControl, NetScaler becomes a single point of configuration.
- Users can be granted access based on EPA checks.

Configuration

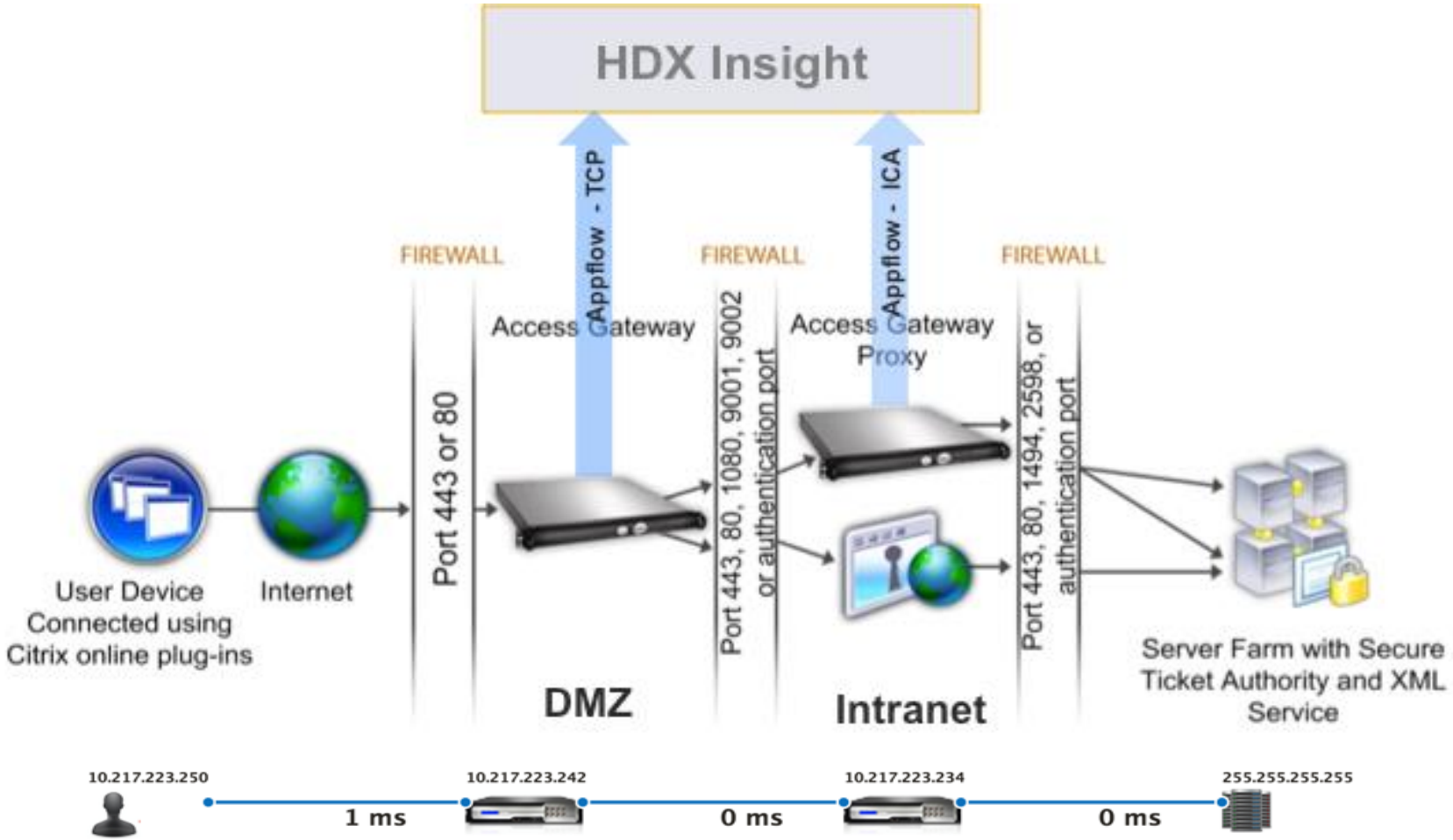


VPN Plugin



EPA Plugin

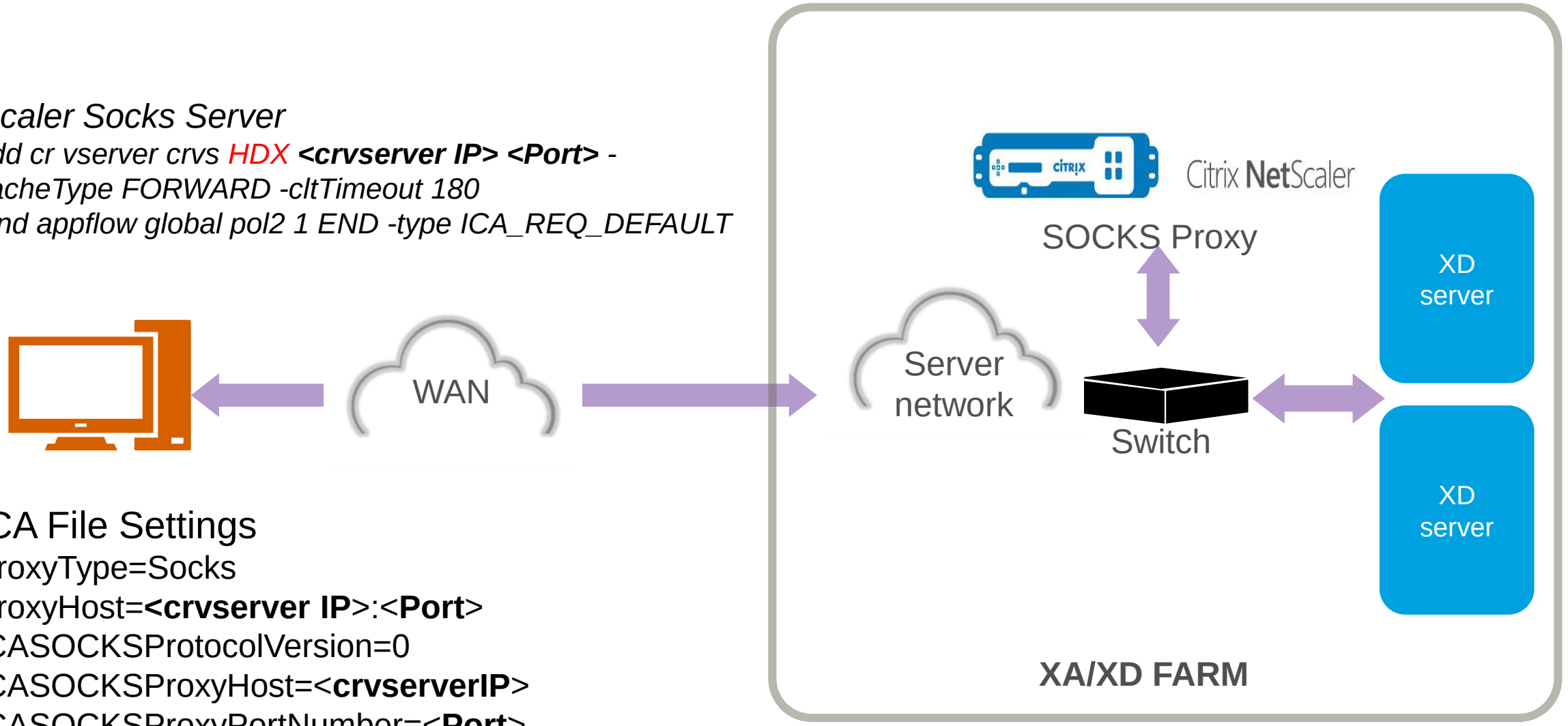
Netscaler Gateway Double Hop Deployment:



HDX Insight LAN User Mode
XenApp XenDesktop SOCKS Proxy

NetScaler Socks Server

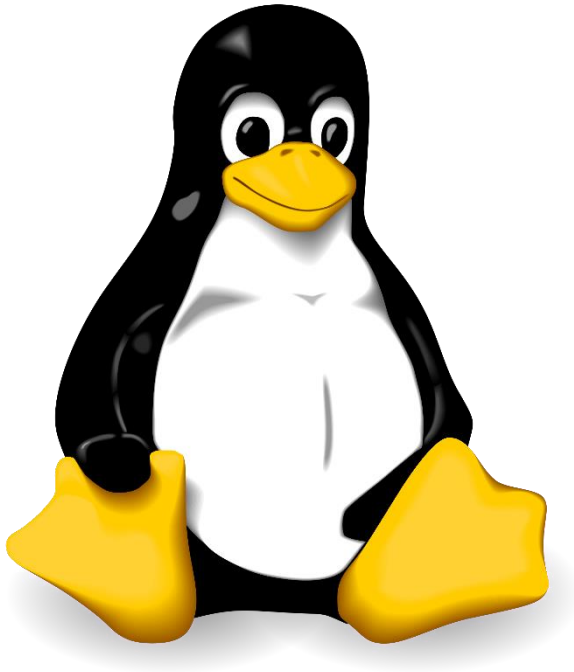
- *add cr vserver crvs HDX* ***<crvserver IP> <Port>*** *- cacheType FORWARD -cltTimeout 180*
- *bind appflow global pol2 1 END -type ICA_REQ_DEFAULT*



ICA File Settings

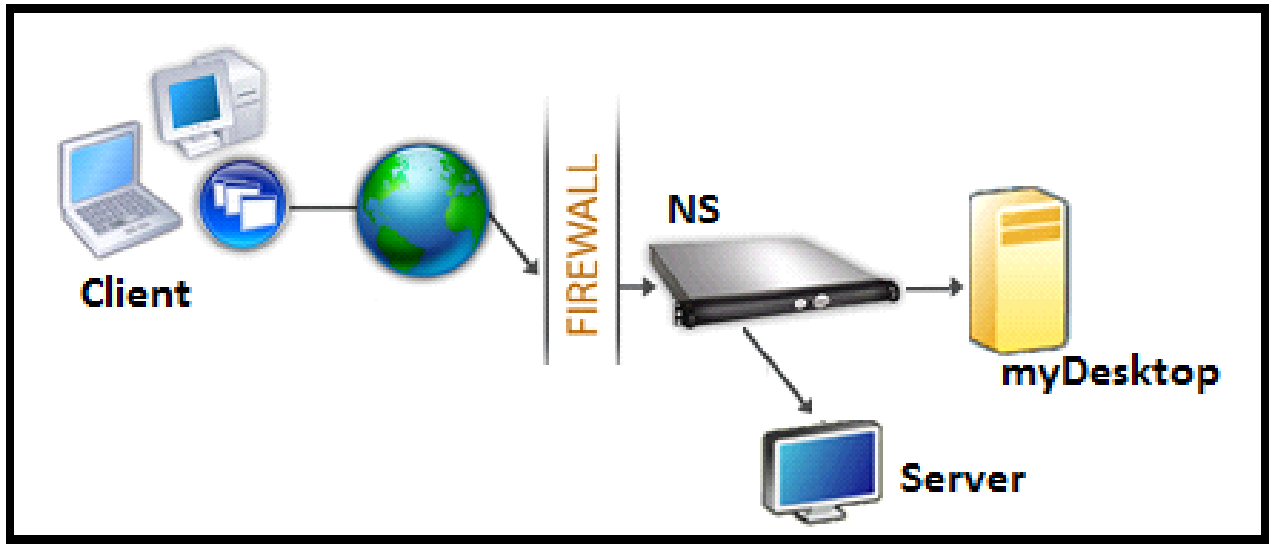
ProxyType=Socks
ProxyHost=**<crvserver IP>**:<**Port**>
ICASOCKSProtocolVersion=0
ICASOCKSProxyHost=<**crvserverIP**>
ICASOCKSProxyPortNumber=<**Port**>

Client Plugins



RDP Proxy in NetScaler Gateway

RDP Proxy Deployment Overview



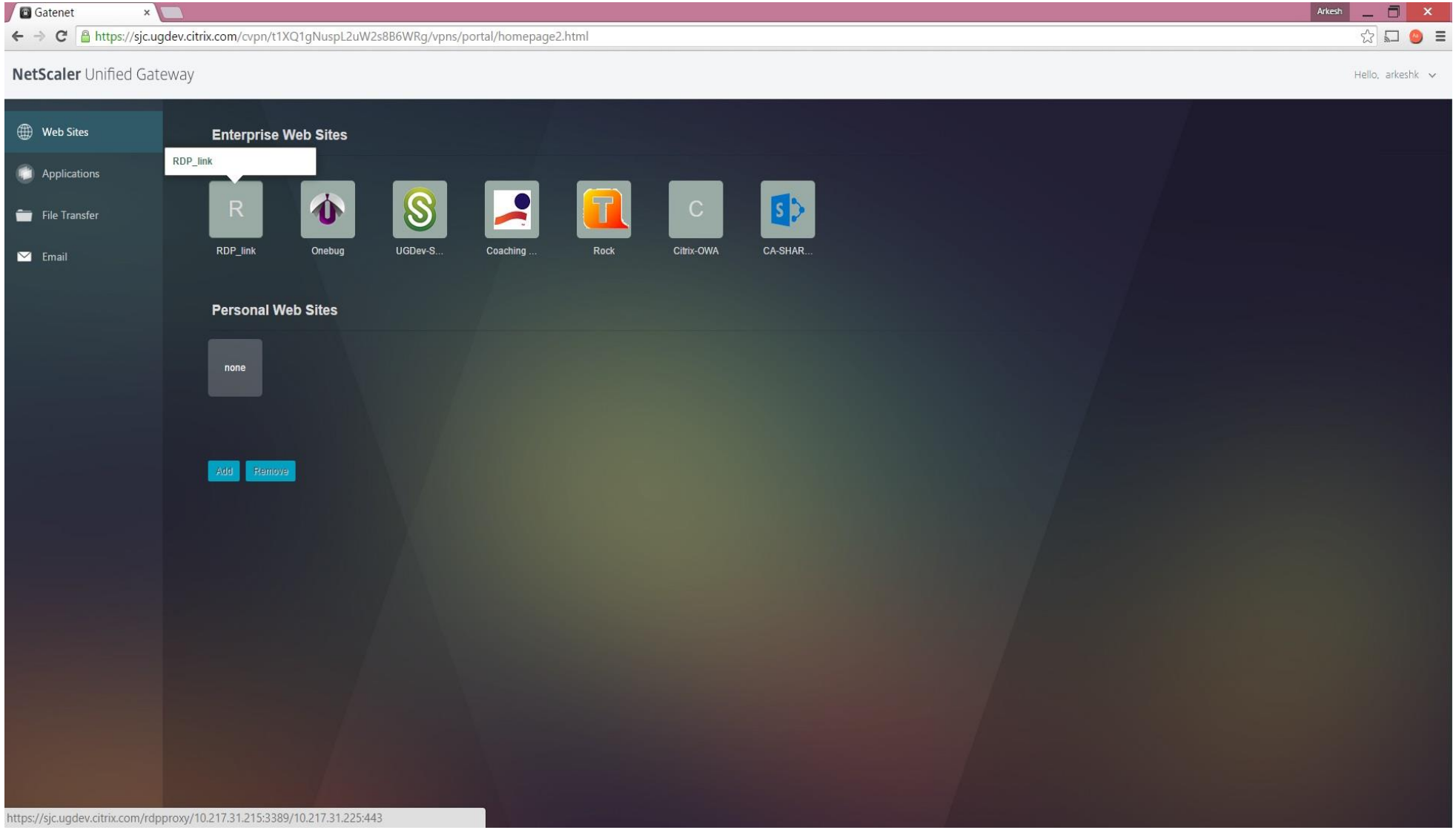
Like a launch.ica

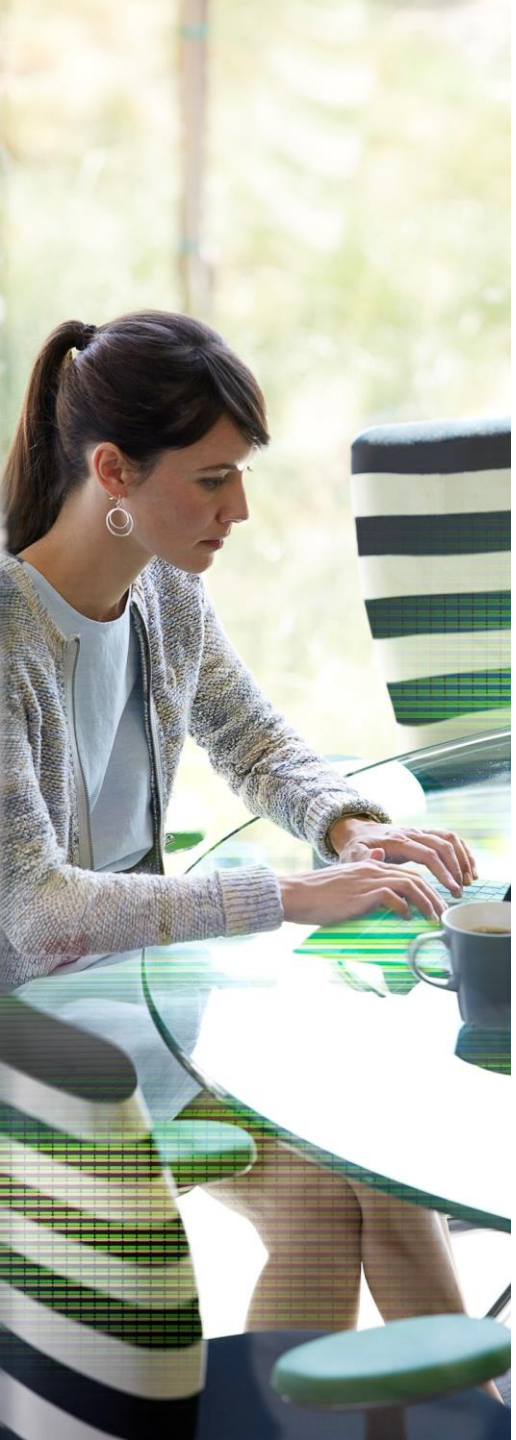
Sample RDP File

full address:s:10.217.31.225:443 [SSLProxyHost field in .ica]

loadbalanceinfo:s:;40;STA209308785;849F5498AFE8C942E8835973F8BFAA
[Address field in .ica]

Portal Page with RDP Resources





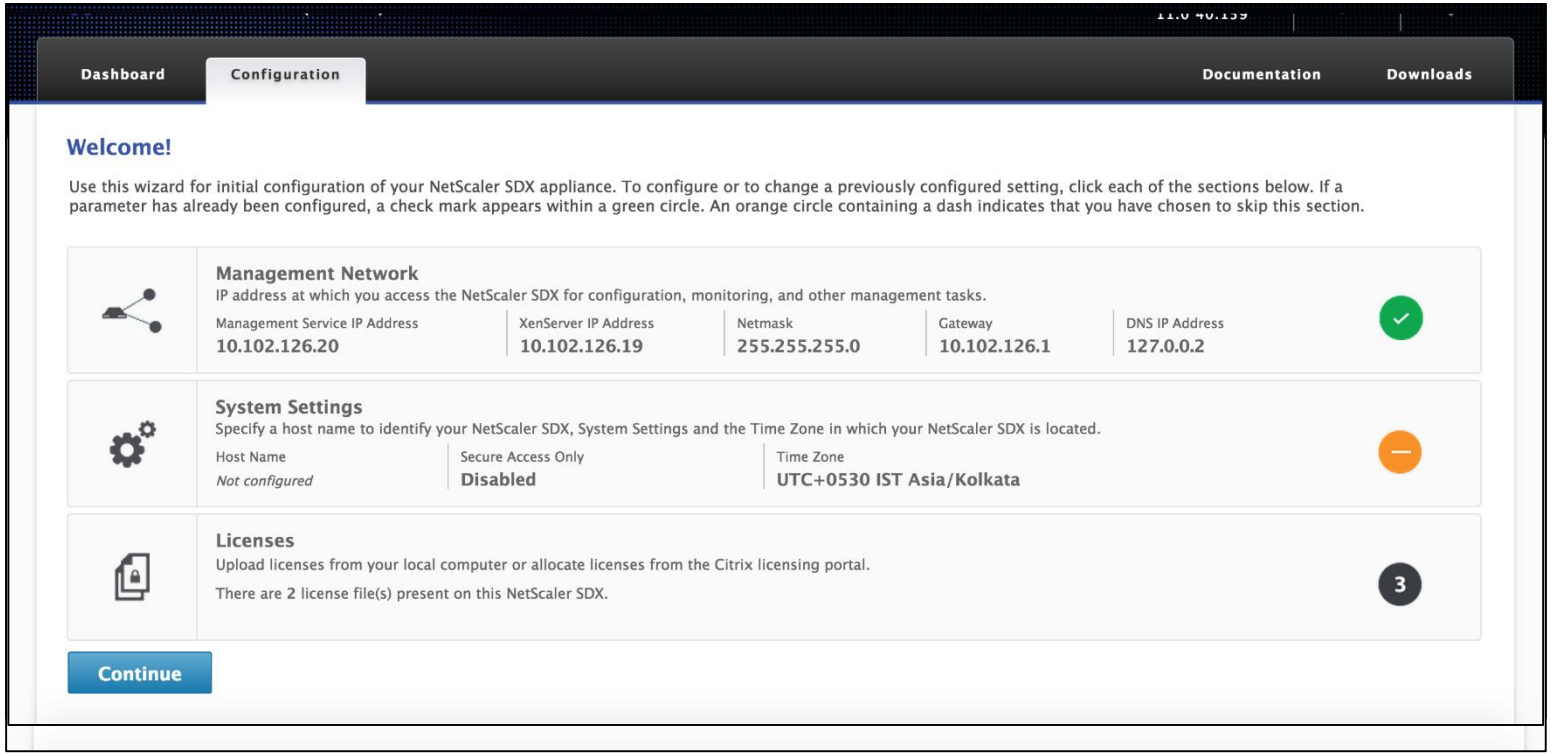
NetScaler 11

SDX

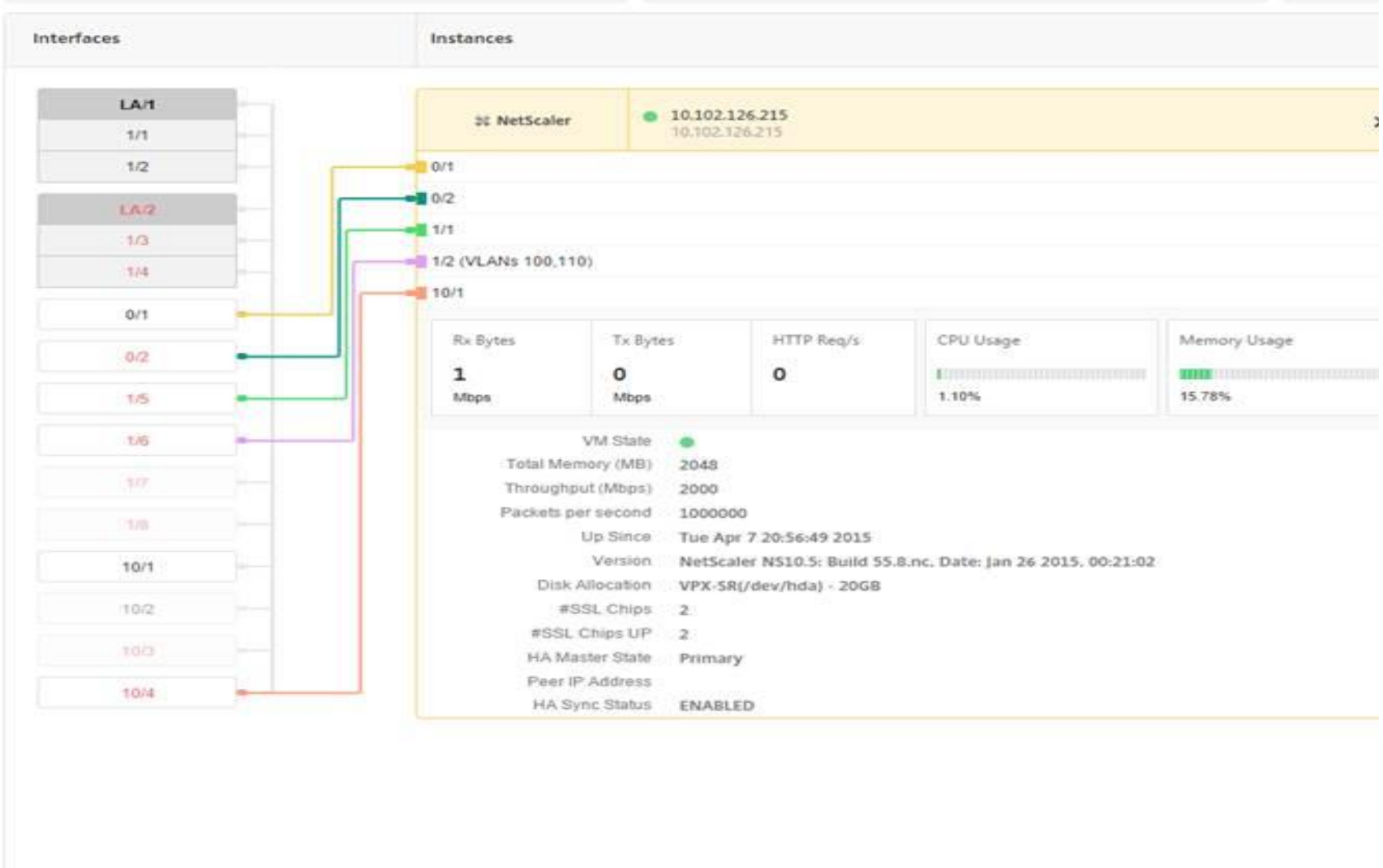
Solution - Simplified Upgrade

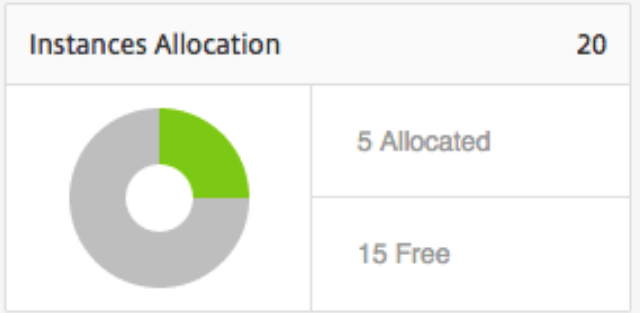
- SDX on Citrix supported matrix - Always
- Single step upgrade of the entire SDX with single image
- Intuitive progress display
- Reduced customer escalations

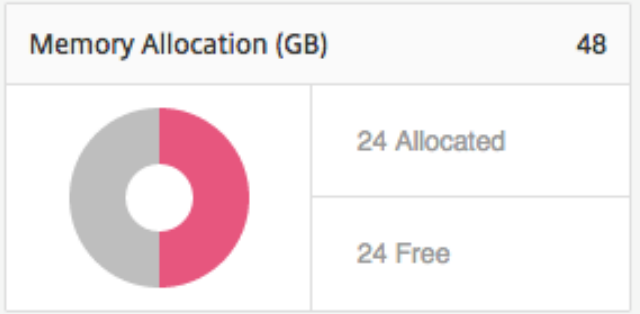
First Time User Experience

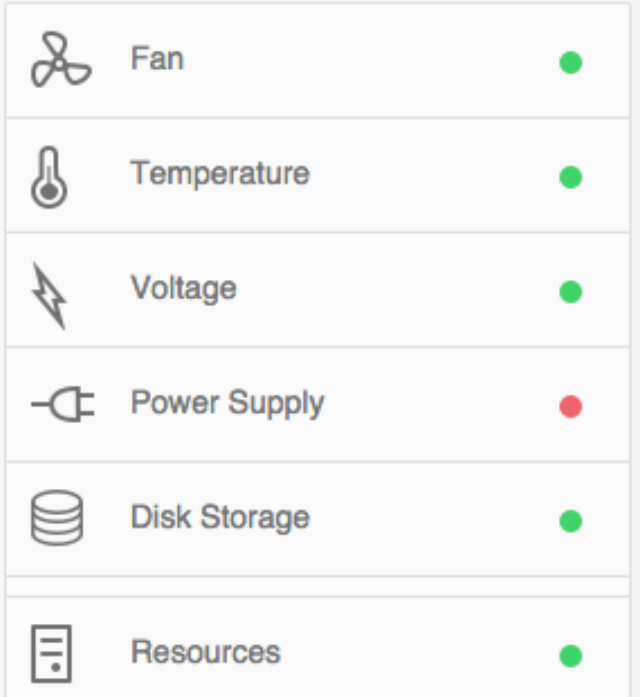


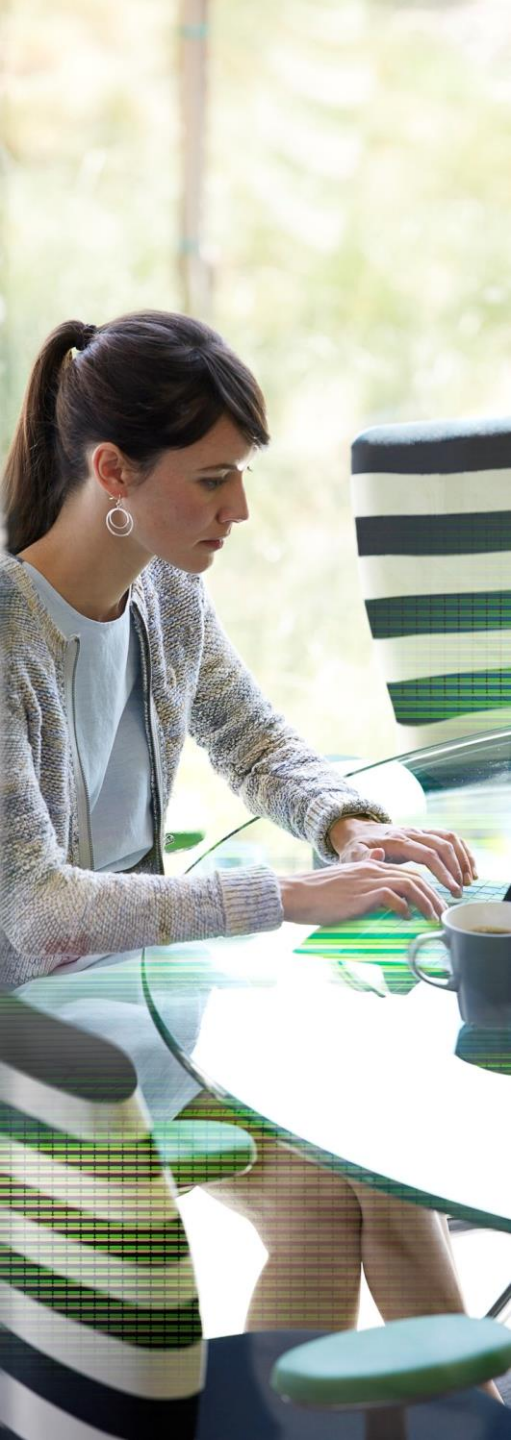
New Dashboard











NetScaler 11

General Improvements

TLS_FALLBCK_SCSV

- Mitigation for POODLE attack
- Prevents attempt to connect to server by downgrading SSL/TLS protocol
- Server identifies if SSLv3 is the highest protocol present on a client by this parameter

Platform	Release Plan
MPX	11.0, 10.5b57
VPX	11.0, 10.5b57
VPX on SDX	11.0, 10.5b57
MPX-FIPS	11.0, 10.5b57

Customize SSL Default Profile

- Edit the default SSL profile to handle global changes to be applied to all of the SSL vservers and services
- Edit the default cipher group bound to the vservers at one location
- Enables to reflect changes to multiple vservers and services by changing configuration at one location
- For example disable SSLv3 globally, remove RC4 from default cipher group

Platform	Release Plan
MPX	11.0, 10.5 MR (Q2, 2015)
VPX	11.0, 10.5 MR (Q2, 2015)
VPX on SDX	11.0, 10.5 MR (Q2, 2015)
MPX-FIPS	11.0, 10.5 MR (Q2, 2015)

New Cipher Support

- AES-GCM/SHA-2
  - Front-end on MPX (PX, N3)
  - TLSv1.2 only.
- ECDHE
  - Back-end on MPX (PX, N3)
  - Note: ECDHE on front-end GA’ed in 10.1, 10.5

- Support on other platforms (FIPS, VPX) coming soon.

PFS Optimizations

- ECDHE: +120%
  - 2 ECC Multiplication + 1 RSA 2K Sign operation.
  - More operations offloaded to Cavium card.
  - Performance with P-256:
    - Corinth-N3: 8,200 TPS (CPU:12%)
    - Decapolis: 65,000 TPS (Expected numbers: Shenick tool limitation, BWC now ready :)
- DHE:
  - DH key generation offloaded to card.
  - Performance with DH-2048bit
    - Corinth-N3:
      - Full PFS (no reuse): 9,200 (CPU:10%)
      - 500 reuse: 15,500 (CPU:11%)

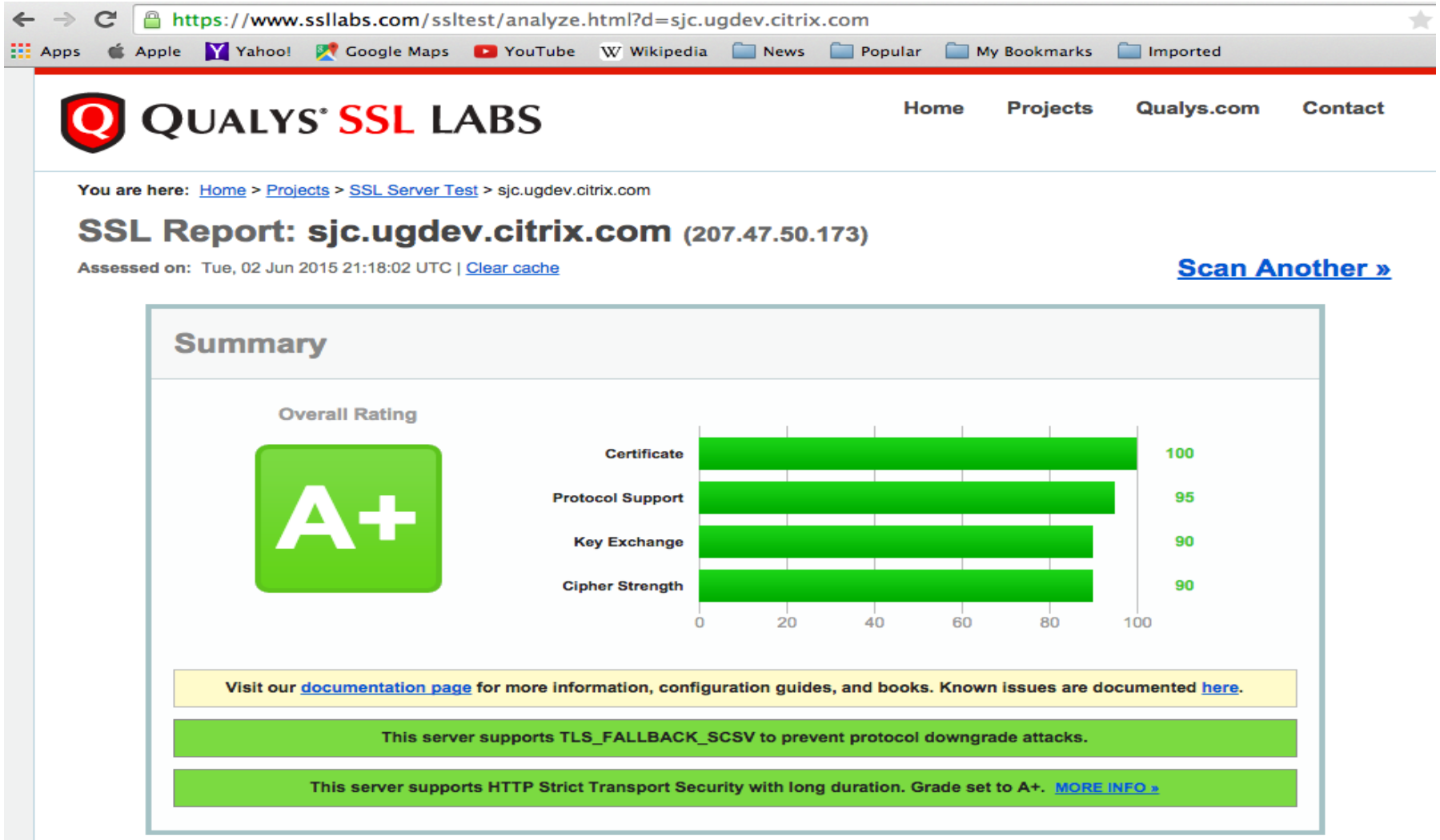
Auto Detection of CertKey Encoding

- NetScaler can now auto-detect the encoding type and load the certificate and key.
  - No need to figure out and give the “–inform” option.
- Supported Formats: PEM, DER, PFX/PKCS#12
- For PFX, with “–bundle” option of “add certkey” command.
  - NetScaler will parse the PFX file.
  - Load the server-cert and server-key
  - Load all the Intermediate-CA certs present in the PFX file
  - Link the certificates.

Protocol Support Matrix for TLSv1.1/1.2

Platforms	Front-End (Vserver)	Back-End (Service)
MPX/SDX	YES [Since 10.0]	YES [11.0, 10.5 (MR – June/July)]
FIPS	YES [11.0, 10.5.e - 55.8007.e]	YES [11.0, 10.5 (MR – June/July)]
VPX	YES [11.0, 10.5 – 57.7]	In-progress [Q3]

Qualys SSL Labs Report: NetScaler MPX/SDX/VPX



http://blogs.citrix.com/2015/05/22/scoring-an-a-at-ssllabs-com-with-citrix-netscaler-the-sequel/

CITRIX®

Secure Cookie Enhancement

Introduction

- When cookie persistence is configured on a lb vserver, for a client request NS insert's a cookie in the response.
- Cookie has information about:
  - Vserver name
  - Ip address & port of service
- Based on which a persistent service is selected on subsequent requests from client containing the cookie.

Vulnerability:

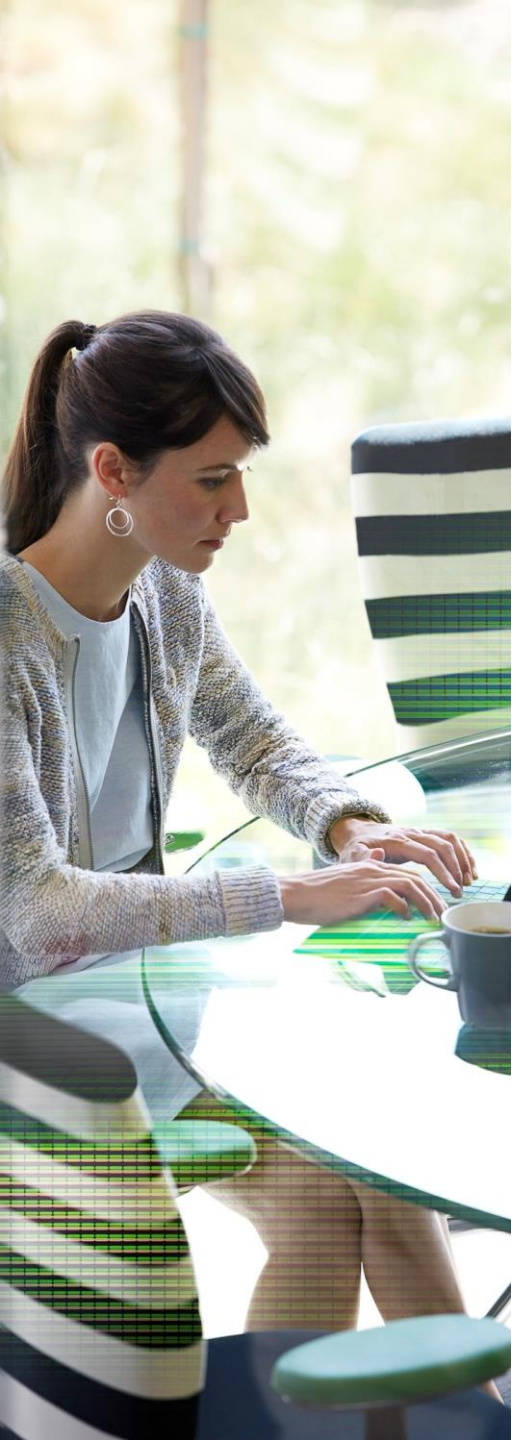
The encoded persistence data can be easily guessed by the attacker exposing backend servers information.

```
 Done
> sh lb param
Global LB parameters:
        Persistence Cookie HttpOnly Flag: ENABLED
        Use Secured Persistence Cookie Flag: DISABLED
        Use Port For Hash LB: YES
        Prefer direct route: YES
        Start RR Factor: 0
        Skip Maxclient for Monitoring: DISABLED
        Monitor Connection Close: FIN
        Use consolidated stats for LeastConnection: YES
        Allow mac mode based vserver to pick thereturn traffic from services: DISABLED
 Done
> sh lb vs v1
        v1 (100.100.100.11:80) - HTTP   Type: ADDRESS
        State: UP
        Last state change was at Wed Mar 25 04:27:15 2015
        Time since last state change: 0 days, 00:28:06.960
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  3 (Total)       3 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state changed to UP
        Mode: IP
        Persistence: COOKIEINSERT (version 0)   Persistence Timeout: 2 min
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
        L2Conn: OFF
        Skip Persistency: None
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
        Mac mode Retain Vlan: DISABLED
        DBS_LB: DISABLED
        Process Local: DISABLED
        Traffic Domain: 0

1) http1 (200.200.200.1: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=ffffffffcbc0d61045525d5f4f58455e445a4a423660
2) http2 (200.200.200.2: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=ffffffffcbc0d61345525d5f4f58455e445a4a423660
3) http3 (200.200.200.3: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=ffffffffcbc0d61245525d5f4f58455e445a4a423660
 Done
> set lb param -UseSecuredPersistenceCookie ENABLED -cookiePassphrase abc
 Done
> sh lb param
Global LB parameters:
```

```
> set lb param -UseSecuredPersistenceCookie ENABLED -cookiePassphrase abc
 Done
> sh lb param
Global LB parameters:
        Persistence Cookie HttpOnly Flag: ENABLED
        Use Secured Persistence Cookie Flag: ENABLED
        Cookie Passphrase: af2b2ce2e894f3210e06b20ddfb0a837
        Use Port For Hash LB: YES
        Prefer direct route: YES
        Start RR Factor: 0
        Skip Maxclient for Monitoring: DISABLED
        Monitor Connection Close: FIN
        Use consolidated stats for LeastConnection: YES
        Allow mac mode based vserver to pick thereturn traffic from services: DISABLED
 Done
> sh lb vs v1
        v1 (100.100.100.11:80) - HTTP   Type: ADDRESS
        State: UP
        Last state change was at Wed Mar 25 04:27:15 2015
        Time since last state change: 0 days, 00:28:25.740
        Effective State: UP
        Client Idle Timeout: 180 sec
        Down state flush: ENABLED
        Disable Primary Vserver On Down : DISABLED
        Appflow logging: ENABLED
        Port Rewrite : DISABLED
        No. of Bound Services :  3 (Total)       3 (Active)
        Configured Method: LEASTCONNECTION
        Current Method: Round Robin, Reason: Bound service's state changed to UP
        Mode: IP
        Persistence: COOKIEINSERT (version 0)   Persistence Timeout: 2 min
        Vserver IP and Port insertion: OFF
        Push: DISABLED  Push VServer:
        Push Multi Clients: NO
        Push Label Rule: none
        L2Conn: OFF
        Skip Persistency: None
        IcmpResponse: PASSIVE
        RHIstate: PASSIVE
        New Service Startup Request Rate: 0 PER_SECOND, Increment Interval: 0
        Mac mode Retain Vlan: DISABLED
        DBS_LB: DISABLED
        Process Local: DISABLED
        Traffic Domain: 0

1) http1 (200.200.200.1: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=14b5a3d92f20893a6e284b5427f5a2d2e6d8522d060272041fa6a13d5ae8e06e7703dbf2
2) http2 (200.200.200.2: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=5ccba3d8a5e8bdd6a14231fabe5f1b5461fde3c3ab805bad730f12ba2798819c58f59989
3) http3 (200.200.200.3: 80) - HTTP State: UP   Weight: 1
        Persistence Cookie Value : NSC_w1=30dfa3db400a9037ac7740ca2934d980a641bebe94c3e6223981c55de6d1856e2eae9657
 Done
>
```

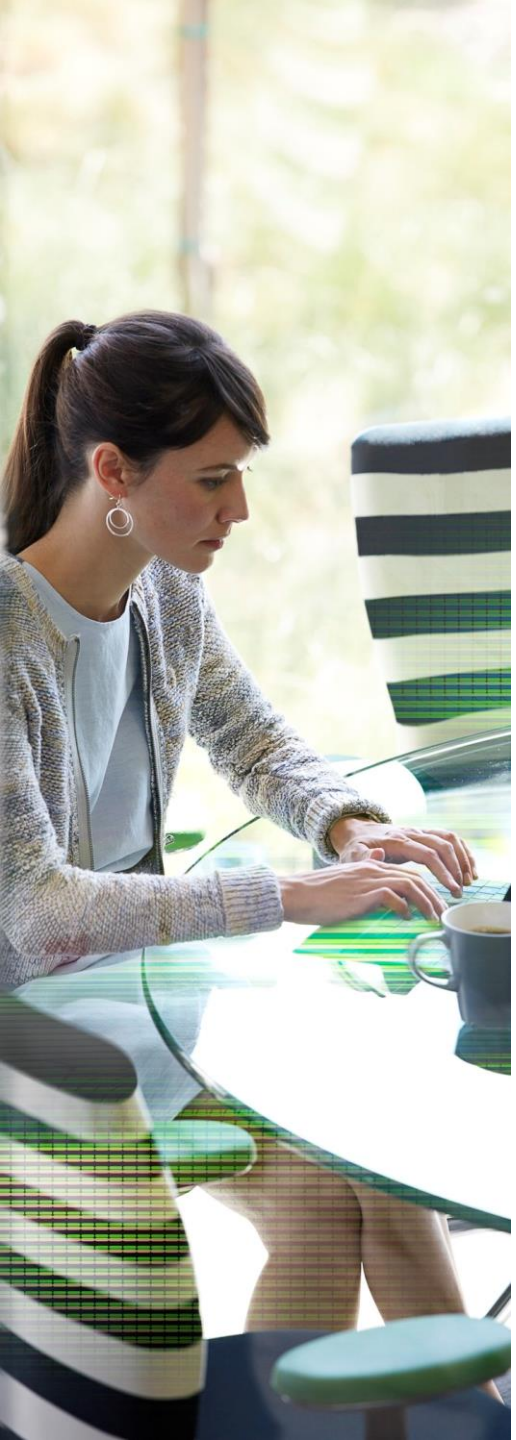


CloudBridge

WAN Optimization 7.4

CloudBridge 7.4.x WAN Optimization

- September:
  - Transparent Caching – Includes authenticated links
  - Thinwire+ support (FP3) – expect **LESS** bandwidth usage than legacy T/W
  - ICA Proxy / NSG sandbox – Acceleration for remote users
- October / November
  - Zero Touch Factory Ship – DHCP / Command Center support
  - Office365 acceleration – Support optimization from local POP
  - SMB3 Optimization – Better pre-fetching and compression
- Q1/2016
  - Session Reconnect – full CGP support
  - Adv. Thinwire / DCR – Better cross session de-duplication



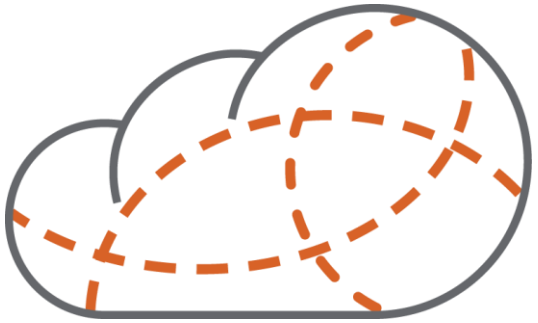
CloudBridge

VirtualWAN – WAN Optimization

CloudBridge

WAN Optimization Solution

Optimize bandwidth while accelerating application delivery



Virtual WAN Solution

Scale bandwidth, ensure availability, and reduce costs

CloudBridge

WAN Optimization Solution

- “Accelerate” the WAN by compressing data and optimizing chatty protocols
- Use when MPLS connections are the only viable WAN option for security or performance reasons

CloudBridge

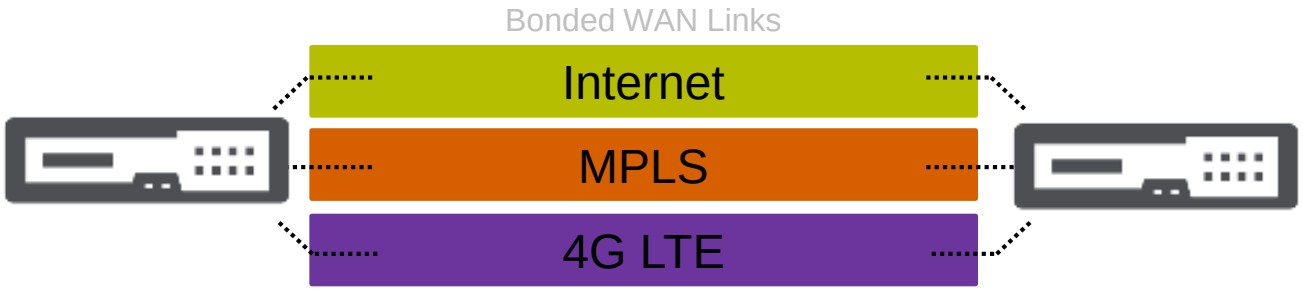
WAN Optimization Solution

Optimize bandwidth while accelerating application delivery

Virtual WAN Solution

Scale bandwidth, ensure availability, and reduce costs

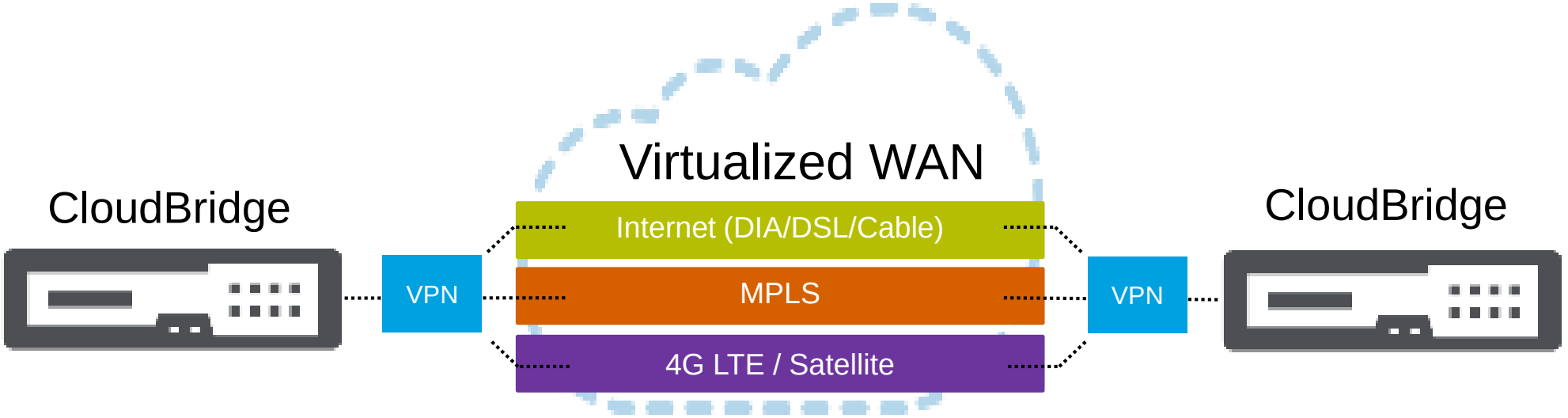
CloudBridge



- Bonds WAN connections for increased throughput
- Use to increase application bandwidth and WAN reliability while prioritizing mission critical apps

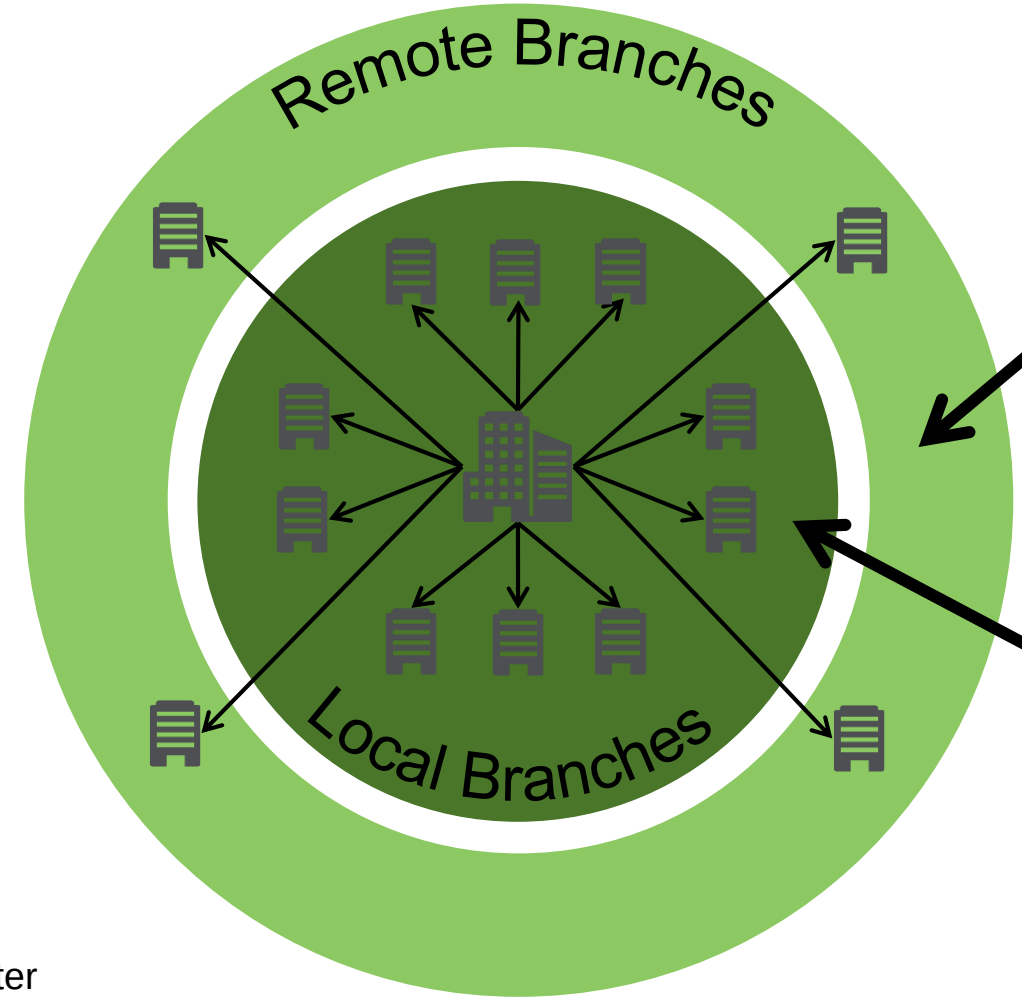
Virtual WAN Solution

CloudBridge Virtual WAN Solution Overview



- Logically bond multiple, distinct WAN connections into one virtual link
- Encrypt paths between devices to provide end-to-end security
- Send packets based upon application needs and link performance

Branch Needs Differ Based Upon Location

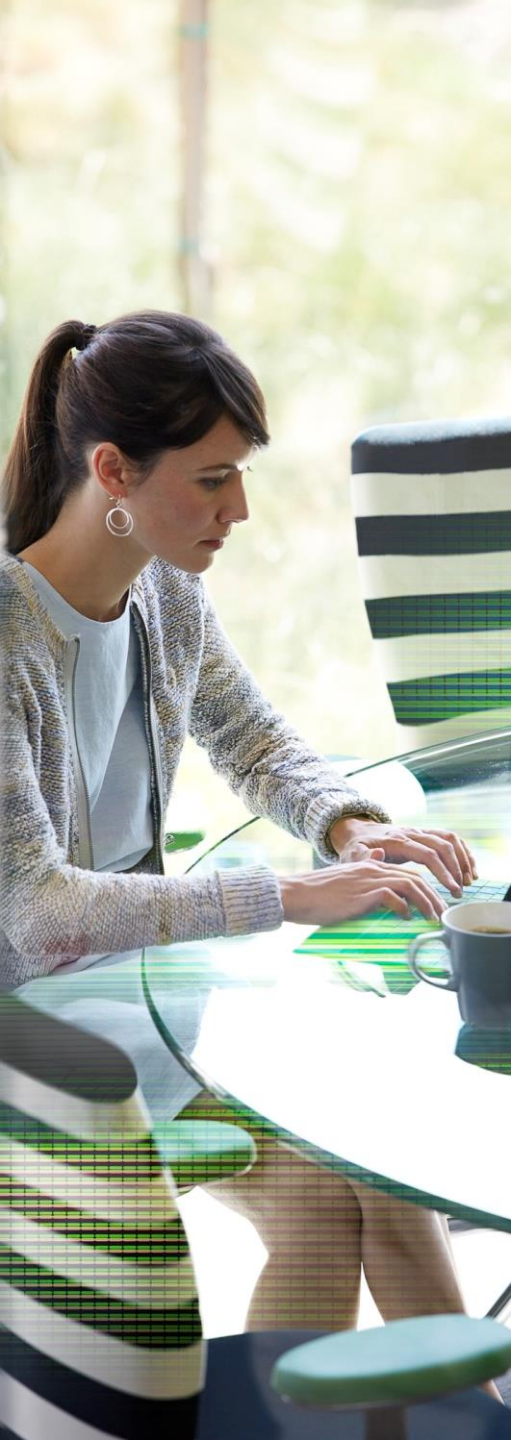


Branch

Data Center

WAN Op Edition

Virtual WAN Edition



CloudBridge

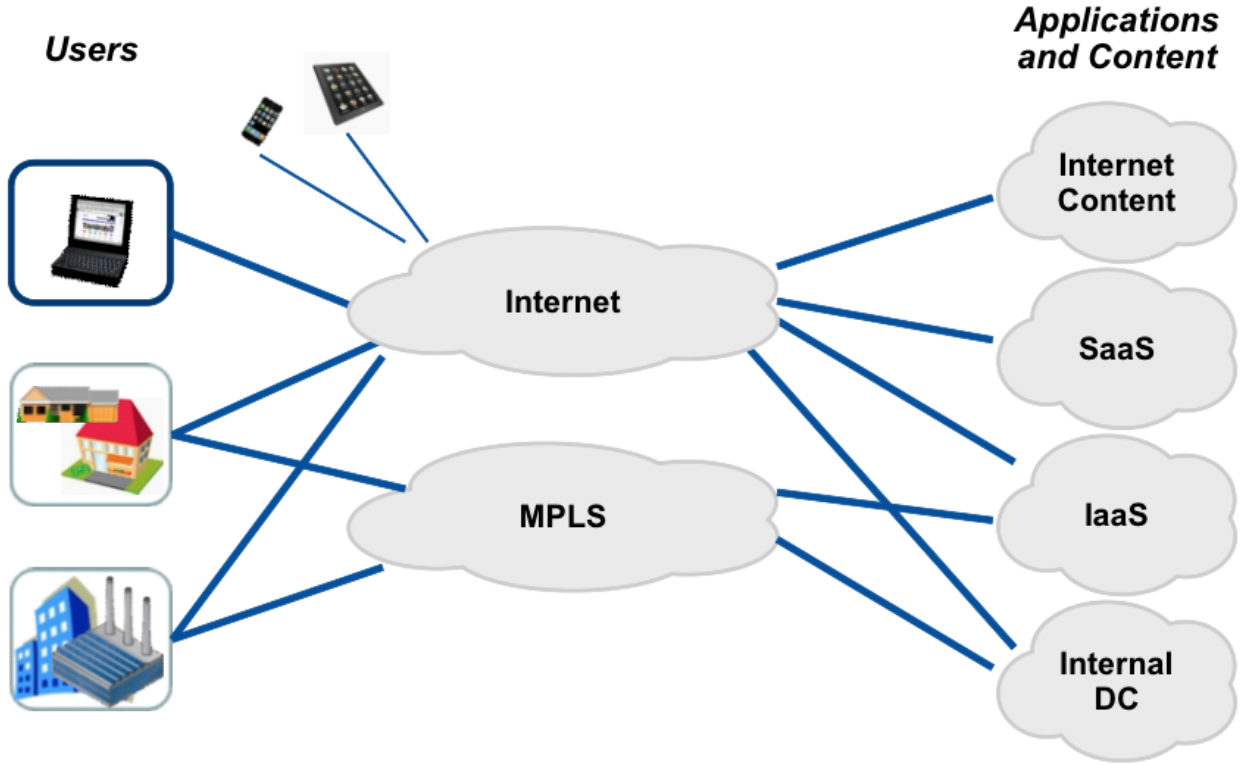
VirtualWAN

Internet and MPLS are both Important

Key recommendation:

"Create a WAN solution that can optimize traffic flows between the Internet and the MPLS for all applications and between both internal and external users."

Gartner Sept 2014



IaaS: infrastructure as a service
DC: data center

Source: Gartner (September 2014)

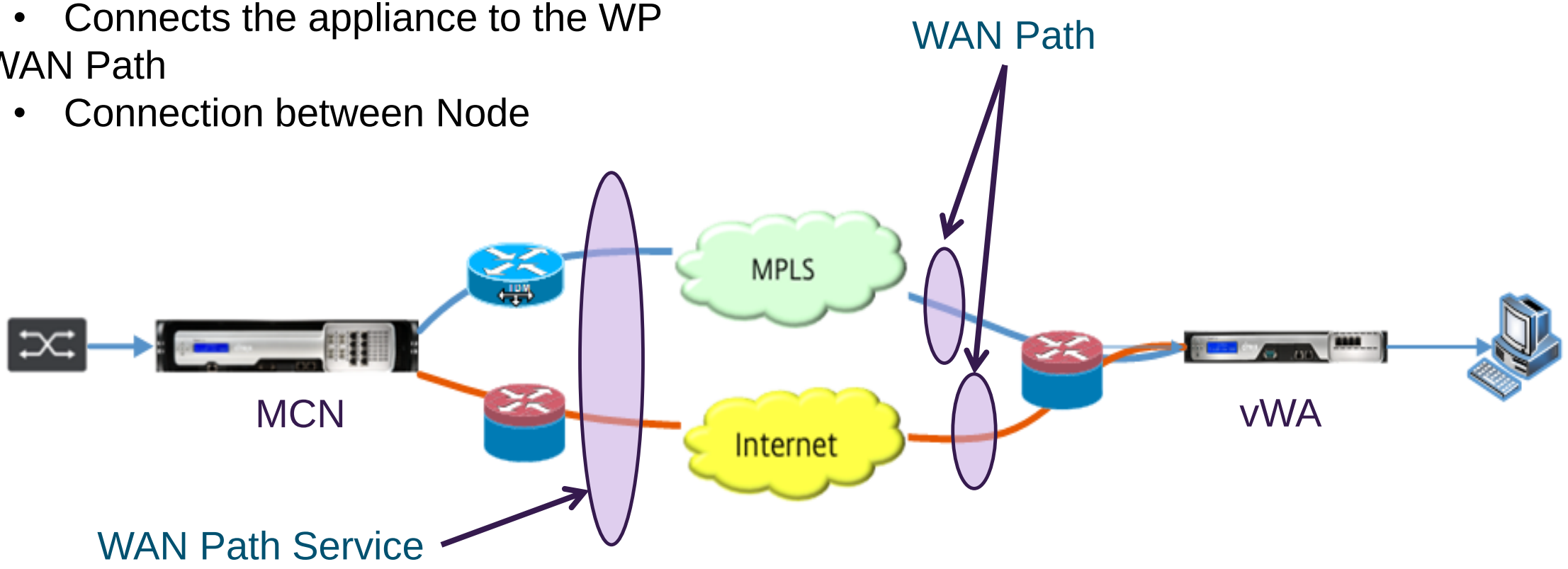
vWAN Architecture Basics

- The Main Control Node (MCN) is the configuration and management node for the Virtual Network.
- Except for the initial install all configuration and management are done here.
- There can be more than one but only one active.

- The vWAN Node (VWN) is located at the Branch sites.
- Very little configuration can be done here

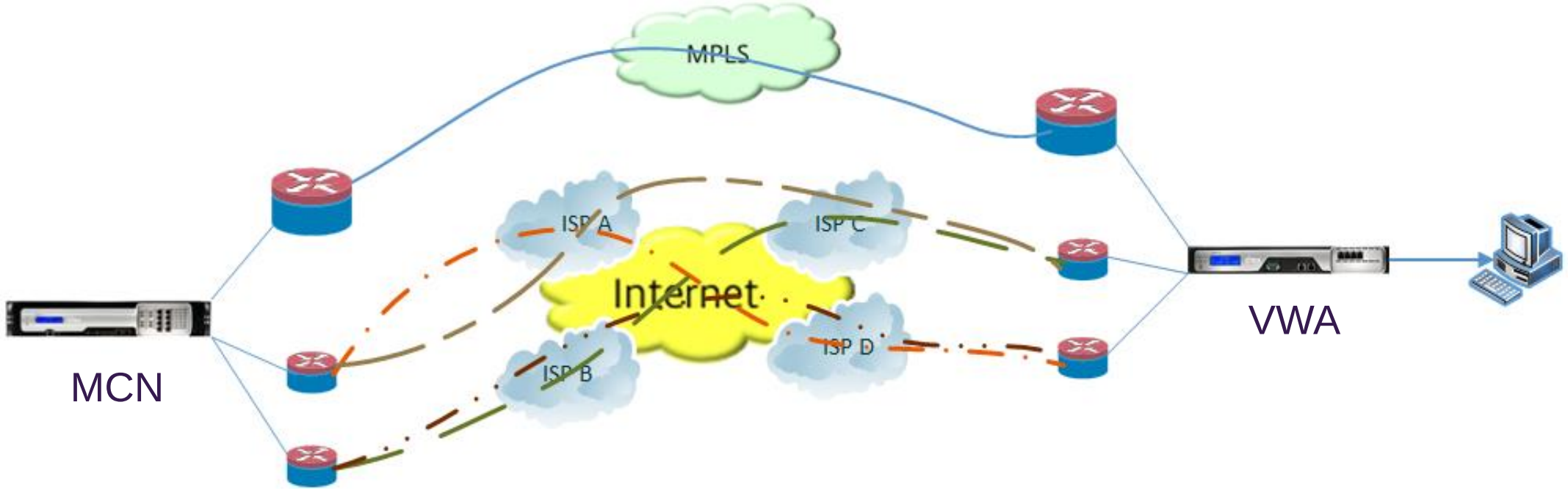
vWAN Architecture Basics

- WAN link
  - Connects the appliance to the WP
- WAN Path
  - Connection between Node



Architecture Basics

- Internet Virtual links
  - Can be path diverse
  - Multiple paths are not affected by single fail point



Flows

Flows are book-keeping devices:

- Flows represent directional flows of traffic across a vWAN
- Flows are created for each Session **in each direction**
- Flows are identified by a 6-tuple of Session information

Flow 6-tuple:

Source IP, Destination IP, Source Port, Destination Port, IP Protocol, DSCP tag (optional)

Virtual WAN is

- Assign App to best path, every packet

Video

XA-Critical

XA-Normal

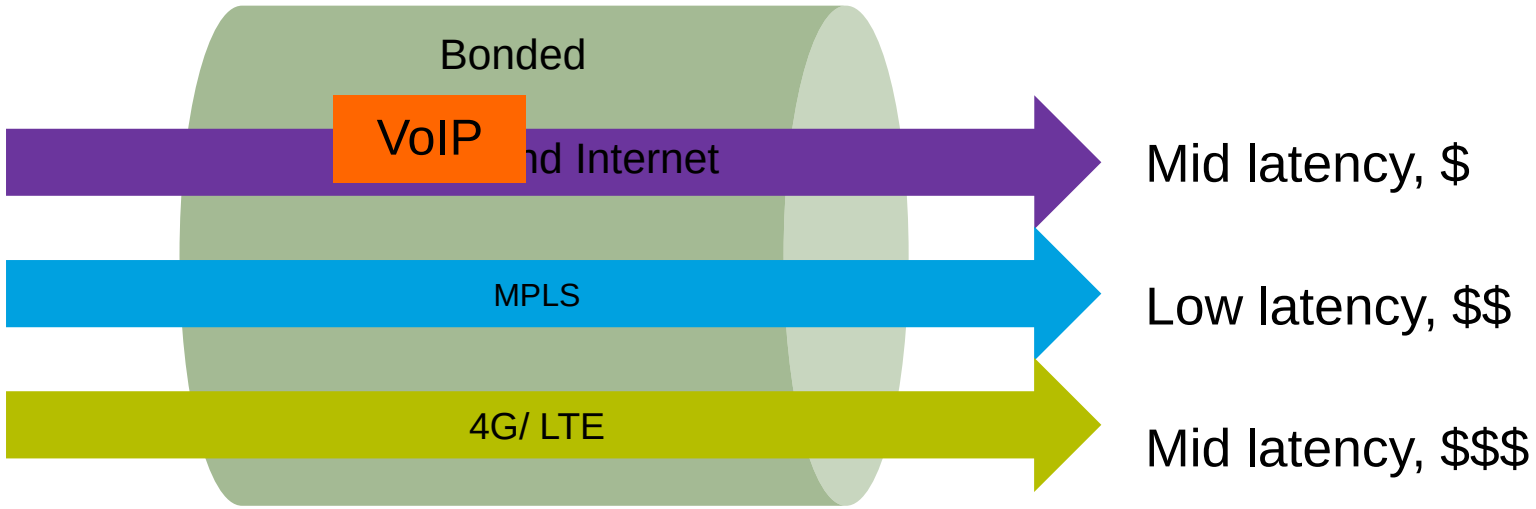
Web

XD

Files

VoIP

Mail

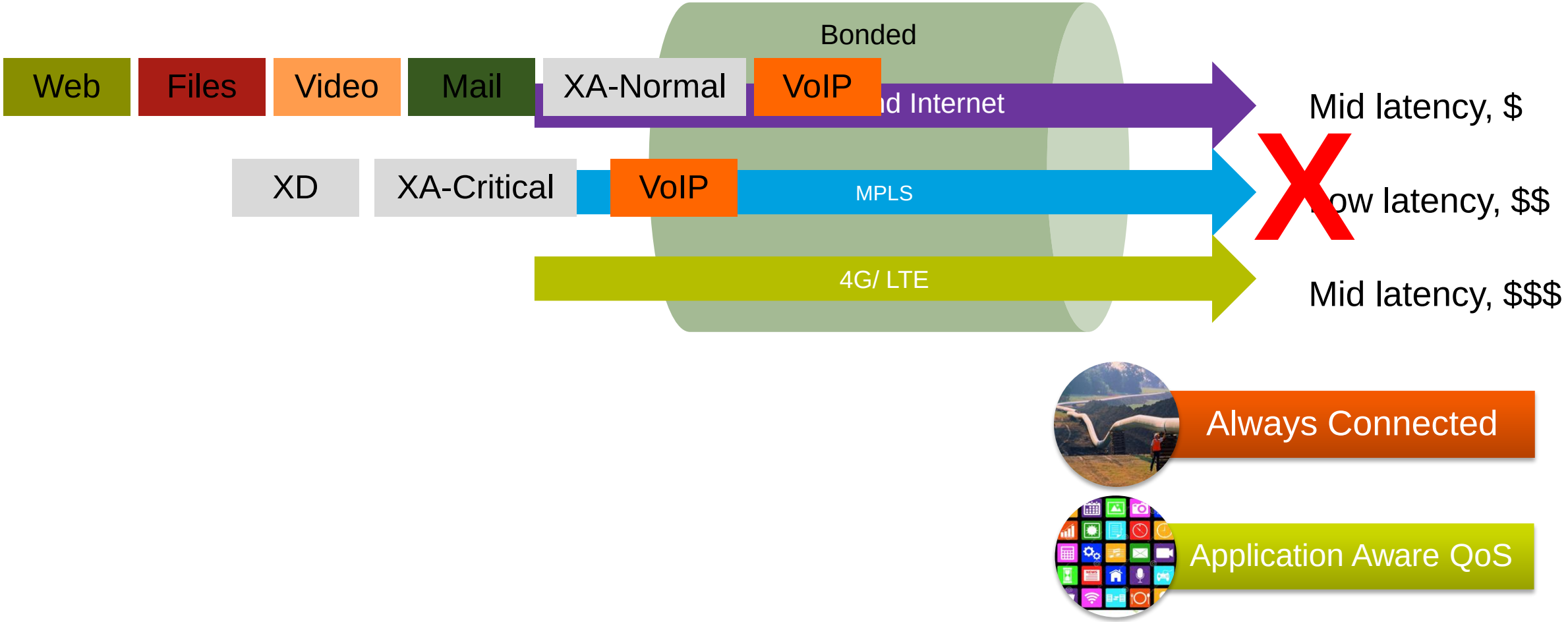


Optimized delivery

Application Aware QoS

Virtual WAN is Always Connected

- Adapt path on network changes



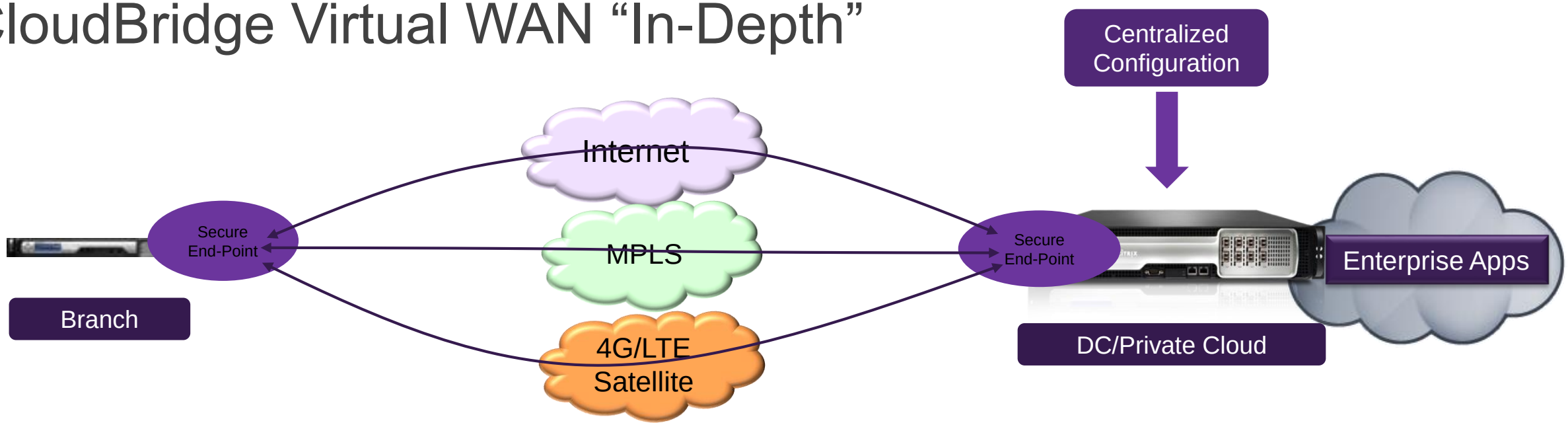
CloudBridge Virtual WAN Solution Leapfrogs the Competition

Criteria	Cisco iWAN	Riverbed	CloudBridge
Path assignment	By connection	By connection	By packet
Adaptation Time	Seconds	Seconds	Milliseconds
Adaptation Methodology	Routing table changes	Device-managed	Device-managed
Adaptation Basis	Round trip	Round trip	Uni-directional
Configuration complexity	Significant	Significant	Minimally invasive & Centralized
Path assessment	Heartbeat-Threshold Driven	Heartbeat-Threshold Drived	Per packet

Why does this matter?

- Granular adaptations → superior end user experience
- Timely adaptations → superior end user experience
- Self contained implementation
- Works just as well with asymmetric networks
- Single point of configuration
- Path selection is based on best available WAN link, not a static threshold being sampled periodically

CloudBridge Virtual WAN “In-Depth”



Key Capabilities

- **Per packet path selection**: Policy based path selection based on packet content
- **Sub-second adaptation**: Reacts in real time to subtle changes in network conditions
- **Packet Duplication**: Improved reliability for sensitive applications across the WAN
- **One-way path selection**: Get maximum benefits for asymmetric network links

CloudBridge VWAN 8.1

Customer Benefits	Supporting Features
Simple Deployment & Licensing	• Quicker branch deployment with VW VPX models • Remote & local licensing for new VW VPX models
Enhanced Manageability & Troubleshooting	• Management of complete Virtual WAN topology • Real-time Alerting • Fault Management & SLA Monitoring
Expanded visibility	• Interactive Network Map • Site-by-site visibility
Increase DC Scale	• Higher capacity SKU for CB 4000 (2Gbps)

CloudBridge Virtual WAN

Virtual WAN VPX Appliances

Feature	VPX 10	VPX 20	VPX 50	VPX 100
Virtualized bandwidth	10 Mbps	20 Mbps	50 Mbps	100 Mbps
Max Virtual Paths	8	8	16	16
Max Dynamic Virtual Paths	2	4	6	8
Max WAN Links (Public/Private)	4/16	4/16	8/32	8/32

Virtual Deployments

Branch

- Upto 100Mbps (Q3’15)
- ESXi, XS and Hyper-V*
- Cisco ISR
- HP branch router*

Virtualized DC

- Starting with 100 Mbps (Q3’15) and going up to 1Gbps*
- ESXi, XS and Hyper-V*

Cloud DC

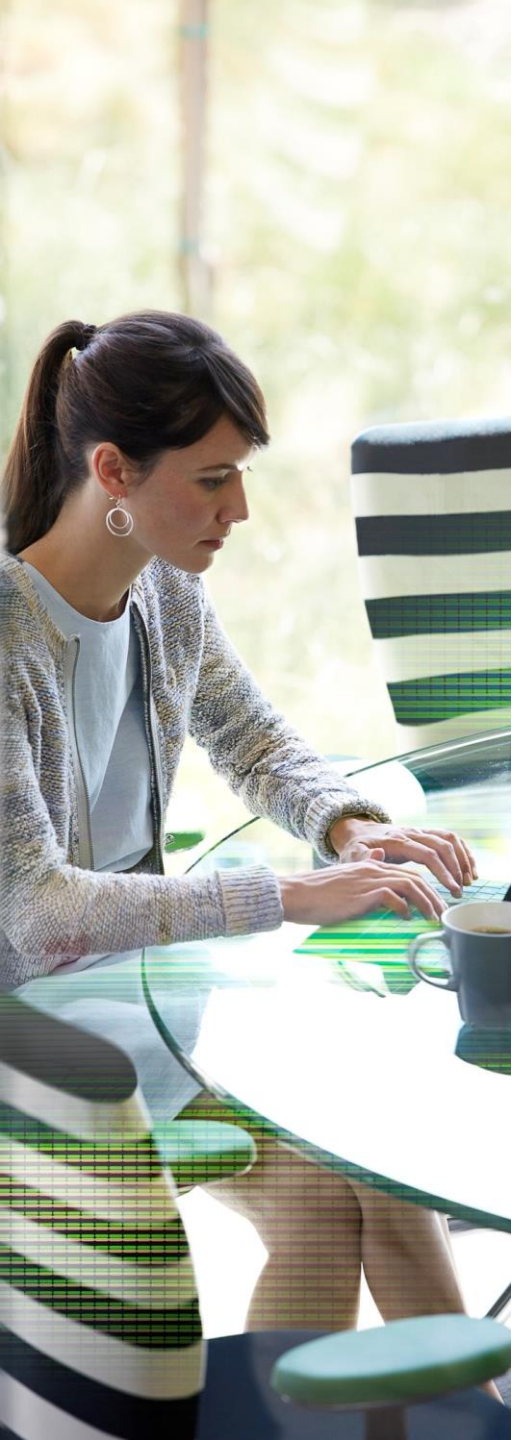
- AWS (Q3’15)
- Azure*
- SoftLayer*

** Target 1H 2016*

Platforms Update

Cirta expands DC platform scalability

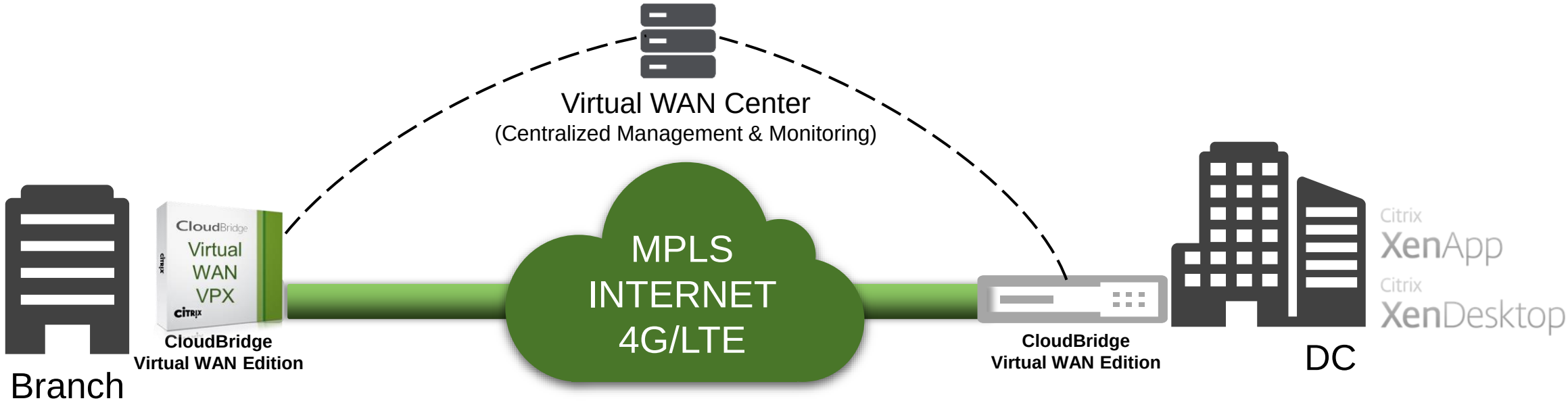
Deployment	Model Series	Bandwidth (Mbps)	Availability
Data Center	CloudBridge 5100	2000-4000	*Q4'15*
	CloudBridge 4000	500-1000 2000	Now
Large Branch / Regional Office	CloudBridge 2000	100-200	Now
Medium Branch Small Branch	CloudBridge 1000	20-100	Now
	CloudBridge 400	10-20	



CloudBridge

VirtualWAN Center

Centralized Management and Monitoring for the Virtual WAN



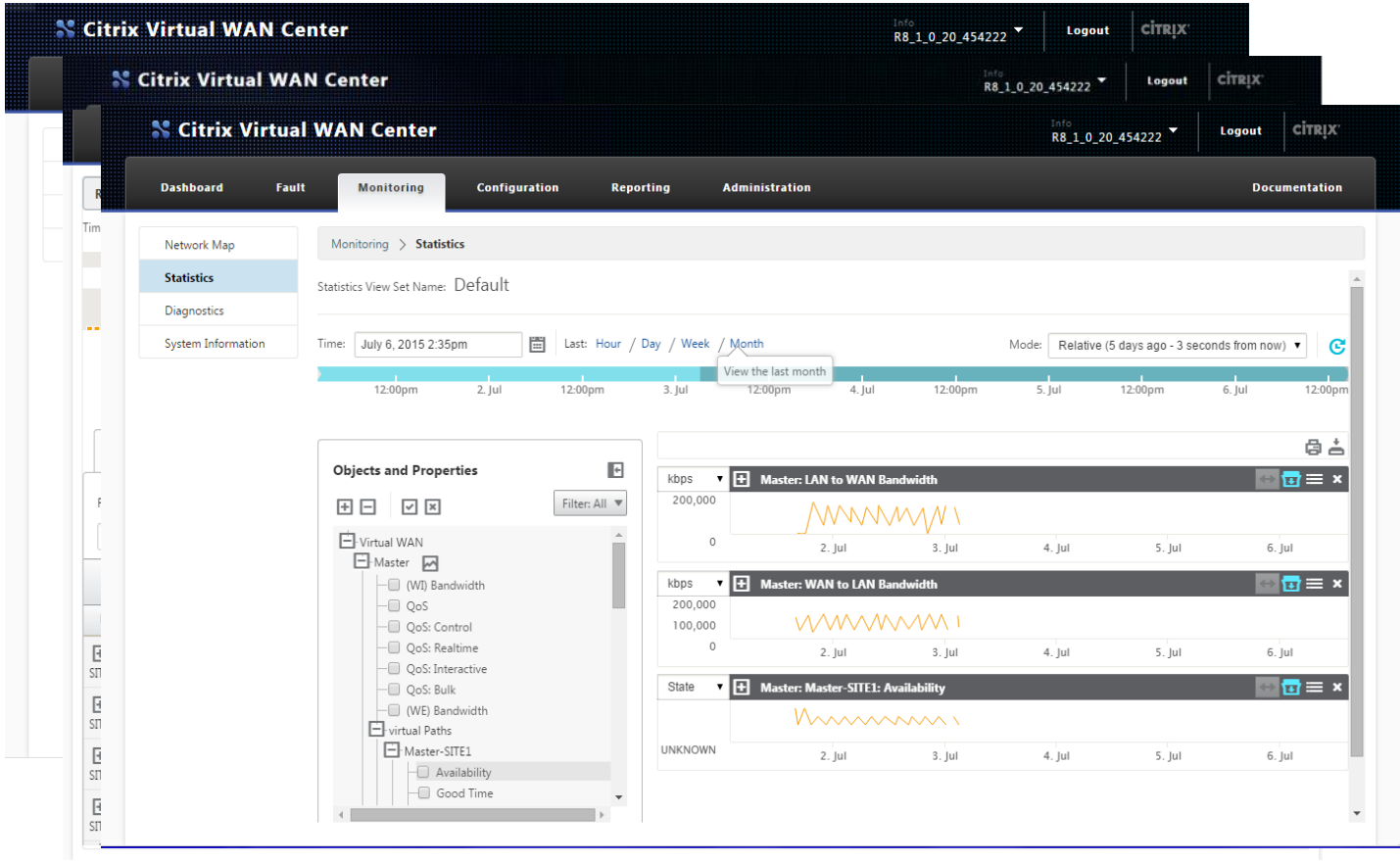
Centralized control with Virtual WAN Center

- Configure
- Monitor
- Analyze / Report

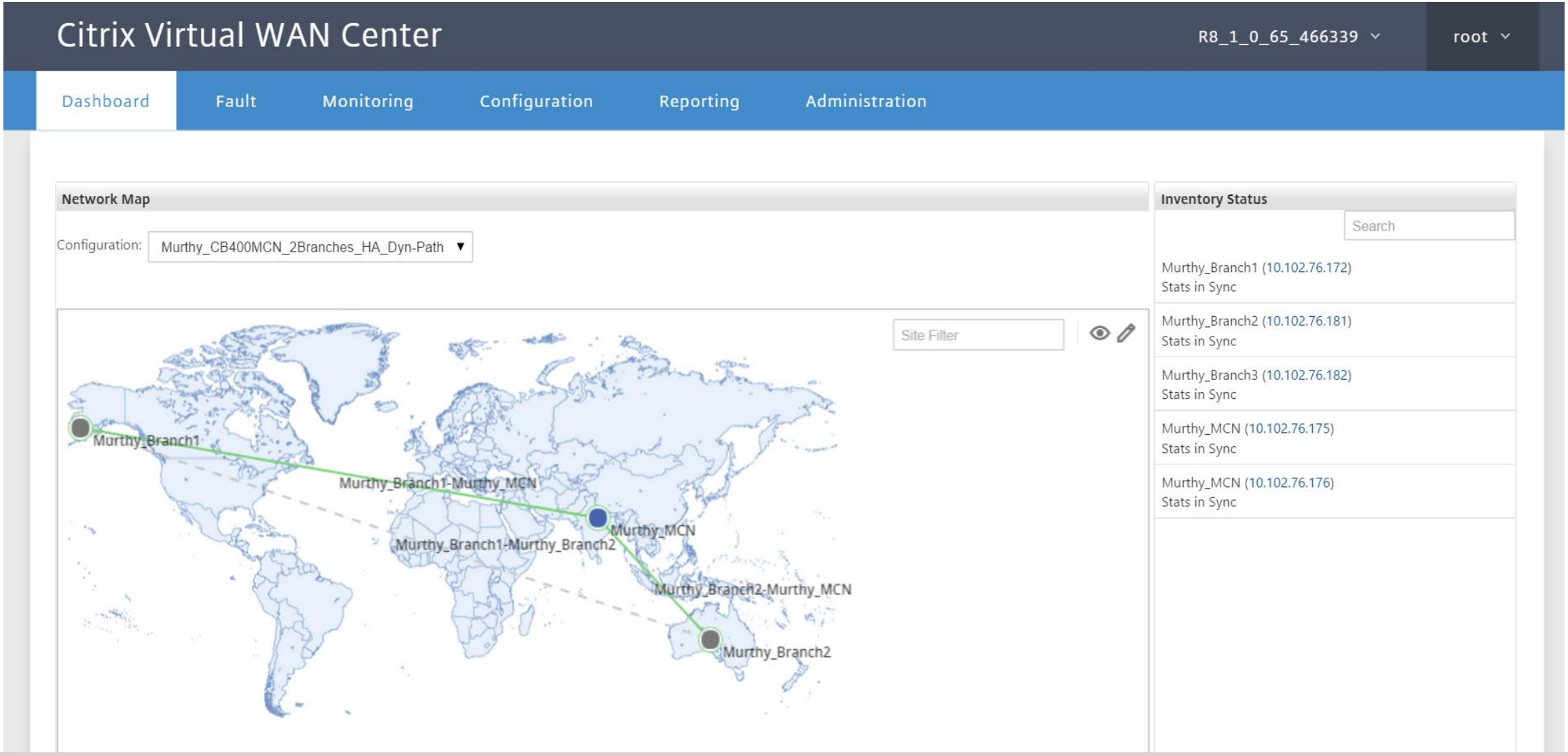
Management / Reporting

Centralized management and monitoring capabilities for the Virtual WAN

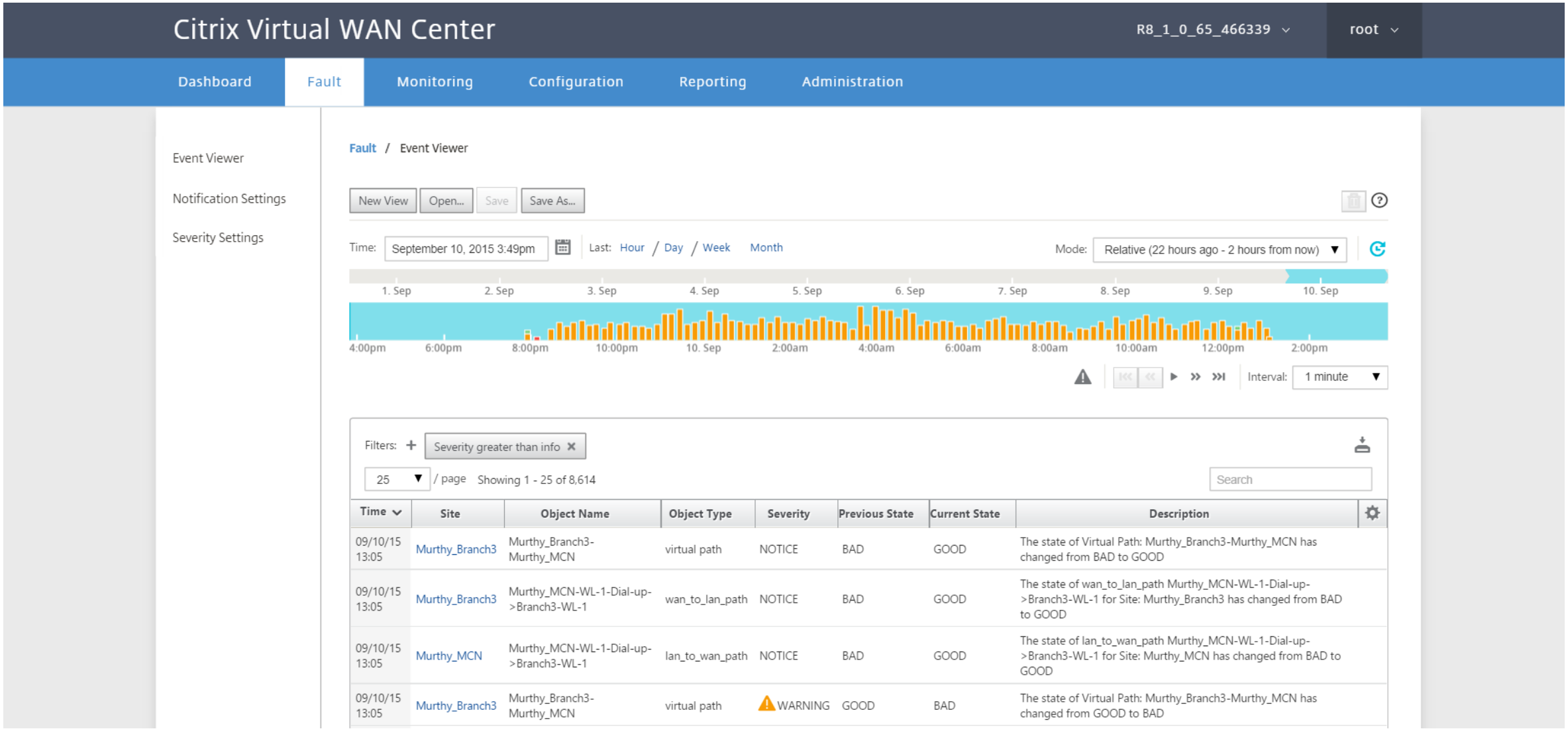
- Centralized, aggregate dashboard view
- Virtual WAN Topology Map
- Proactive SLA Monitoring for WAN links
- Fault Management and Alerting capabilities



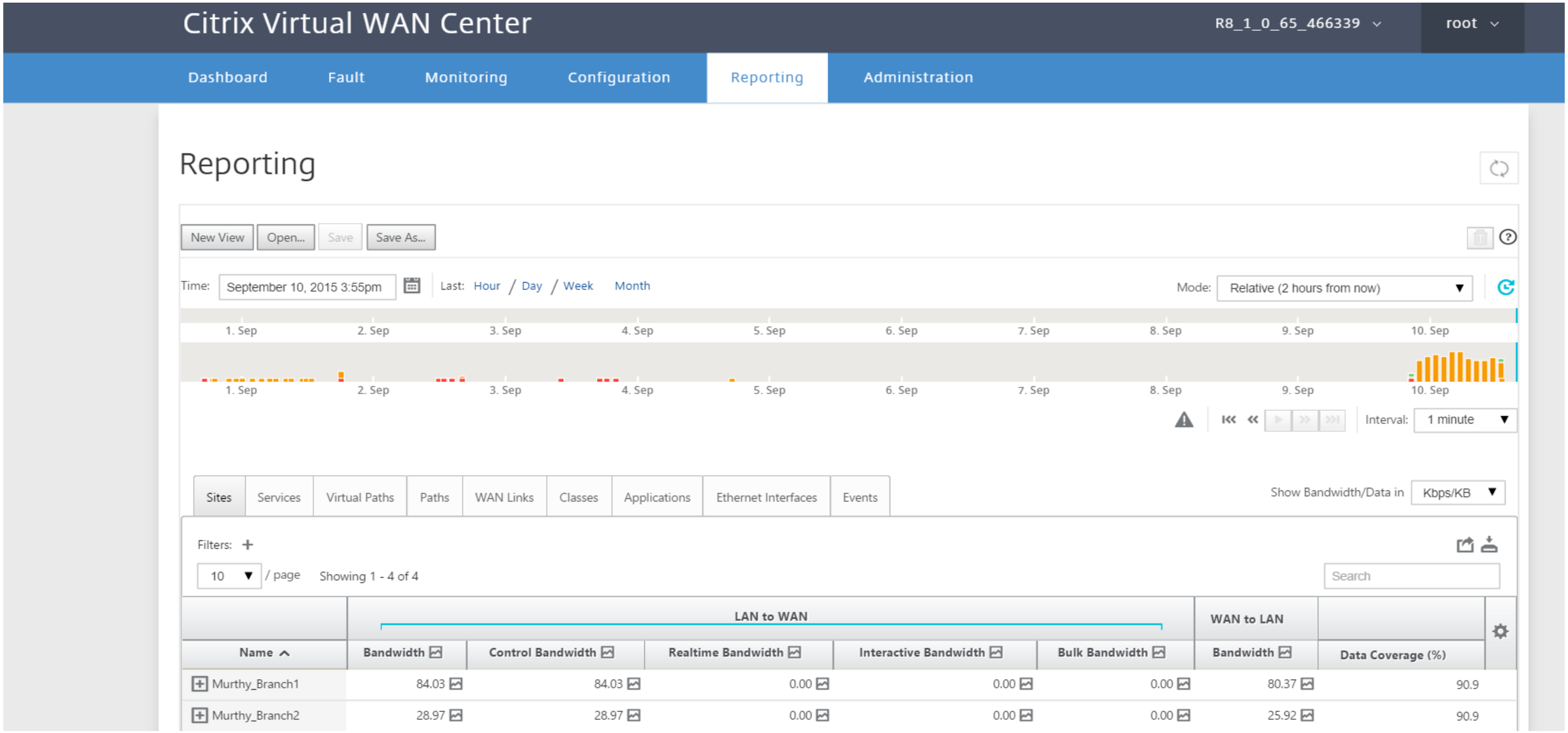
Virtual WAN Centre Dashboard

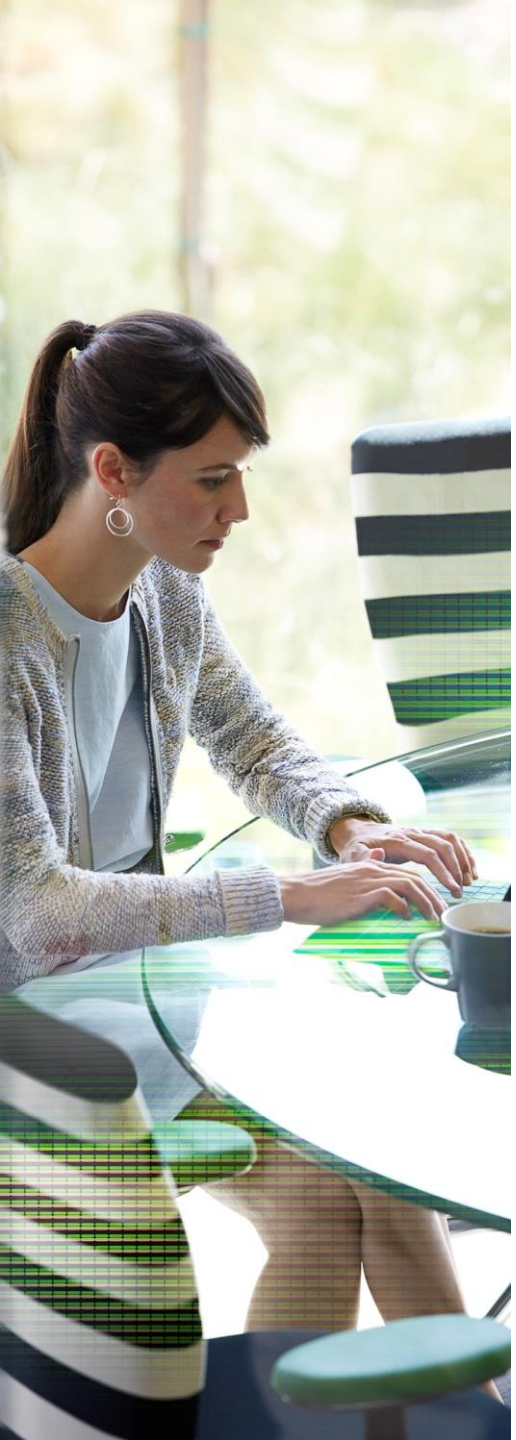


Virtual WAN Centre Fault Management



Virtual WAN Centre Reporting





CloudBridge

HDX Optimizations

The three HDX display modes

Desktop Composition Redirection (DCR)

Advanced Thinwire (H.264)

Thinwire+ (Snowball)

Desktop Composition Redirection (DCR)

- Uses Direct 3D to render the screen -- replaces GDI-based screen handling
- Offers the best screen user experience – Aero-like view
- Offloads screen rasterization to the client – best server scalability
- Good cross-session deduplication (better compression)
- BUT
- Uses a lot of bandwidth
- Only supported by Windows 8+ and Server 2012
- May not be the long-term solution – e.g., Linux VDA, etc.

Advanced Thinwire (H.264)

- Very efficient compression, especially for server-rendered video, graphic apps
- Efficient rasterization on the server
- Wide support for various operating systems (Windows, Linux, etc.)

BUT

Does not de-duplicate well (20% versus 50% to 80%)

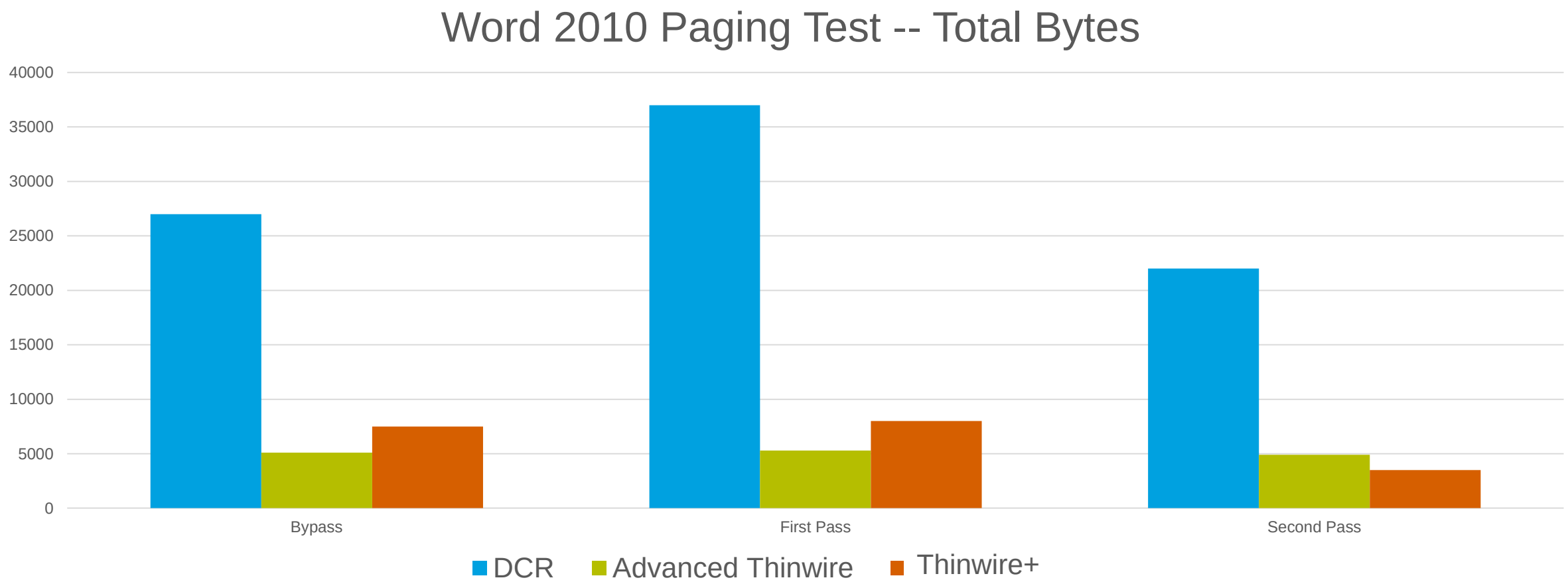
Server is not as scalable as DCR

Best for graphics applications, less applicable for general user apps (SAP, Office)

Thinwire+ (Snowball)

- Highly efficient use of bandwidth
- Broad cross-platform support
- High cross-session de-duplication
- Rasterizes on the server -- about the same efficiency as Advanced Thinwire
- BUT
- Not as good as Advanced Thinwire for video and heavy graphics apps
- Not as scalable as DCR on the server

How much bandwidth does each consume with and without CB?



Which to choose?

- WAN Implementations:
  - Use Thinwire+ with CloudBridge for highest bandwidth efficiency
  - Advanced Thinwire for server rendered video
  - Modified DCR template for the best user experience
- LAN Implementations
  - Local implementations use Advanced Thinwire or DCR
  - CAD use HDX 3D Pro (Adv. Thinwire)
  - Server rendered video use advanced Thinwire
  - Only use legacy Thinwire for compatibility with XP and older thin clients

XenDesktop / App are perfect for Virtual WAN) ADSL & Cable

Work better. Live better.