Notes from the lab: NetScaler Secure Web Gateway

Finally had some time to test the new forward proxy functionality with the newly released NetScaler Secure Web Gateway, and that meant a new blog.

First things first all the information needed to deploy NetScaler Secure Web Gateway

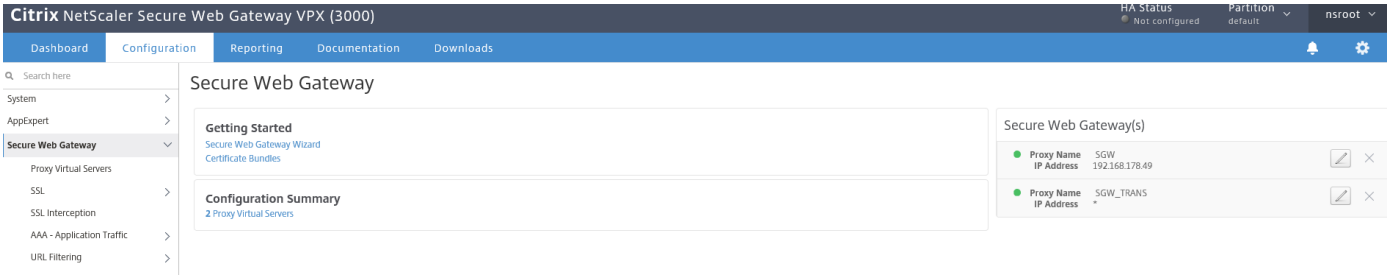
Documentation:
http://docs.citrix.com/en-us/netscaler-secure-web-gateway/12.html

Downloads:
https://www.citrix.com/downloads/netscaler-adc/ (it's the same appliance as the normal NetScaler ADC only locked down at the moment with the dedicated licenses for Secure Web Gateway and URL threat intelligence subscription. Sadly we cannot mix and match it just yet with the platform license. I believe this is an RFE for the end of this year)
https://www.citrix.com/downloads/netscaler-mas/ for the logging and visibility of outbound traffic and transactions

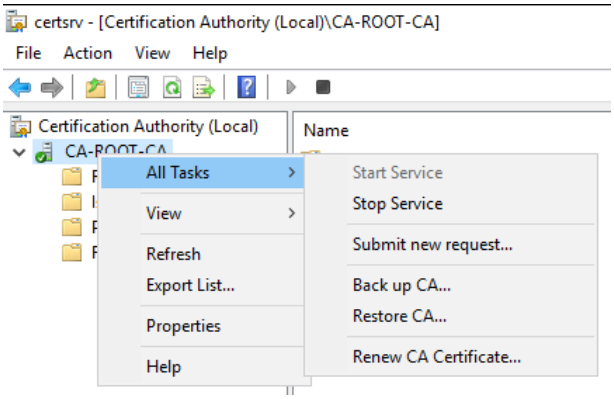
Licenses:
The following partner demo licenses can be allocated, I had help from the local Citrix Sales Engineer regarding allocation that will definitely safe you time.
Citrix Netscaler VPX 3000 Secure Web Gateway Edition - Eval 90 days
URL Threat Intelligence for MPX 5901, 5905, 8905 and VPX 200, 1000, 3000, 5000 , 90 Days

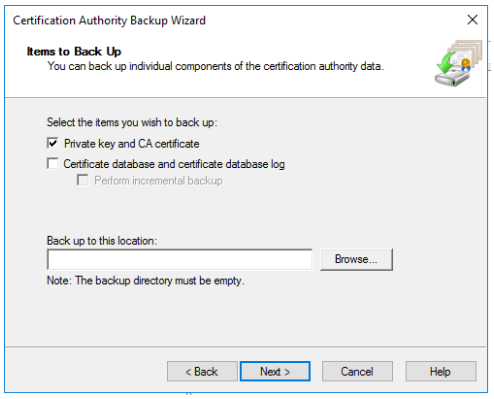
After download and import the allocation and installation of license files and basic setup is the same as any other NetScaler appliance.

And then it's time to run the wizard:



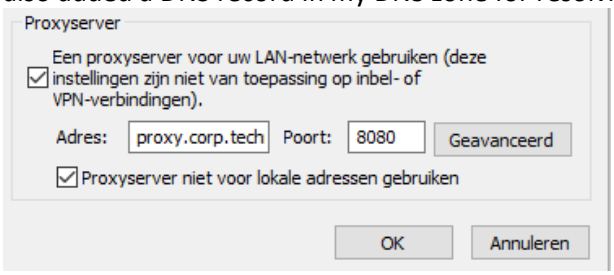
I've followed the "Use Case: Making Enterprise Internet Access Compliant and Secure" from the above link from docs.citrix.com and it's pretty much self-explanatory. The only caveat I found was with my internal Active Directory Certificate Services (ADCS) as Root CA. The proxy will need the **private** key of your CA to sign/intercept all the traffic. See the following figures for that process:





Afterwards import this certificate as a Root certificate on the NetScaler, I first installed it locally on my machine and exported it as PFX (because of the conversion on the NetScaler to PEM format)

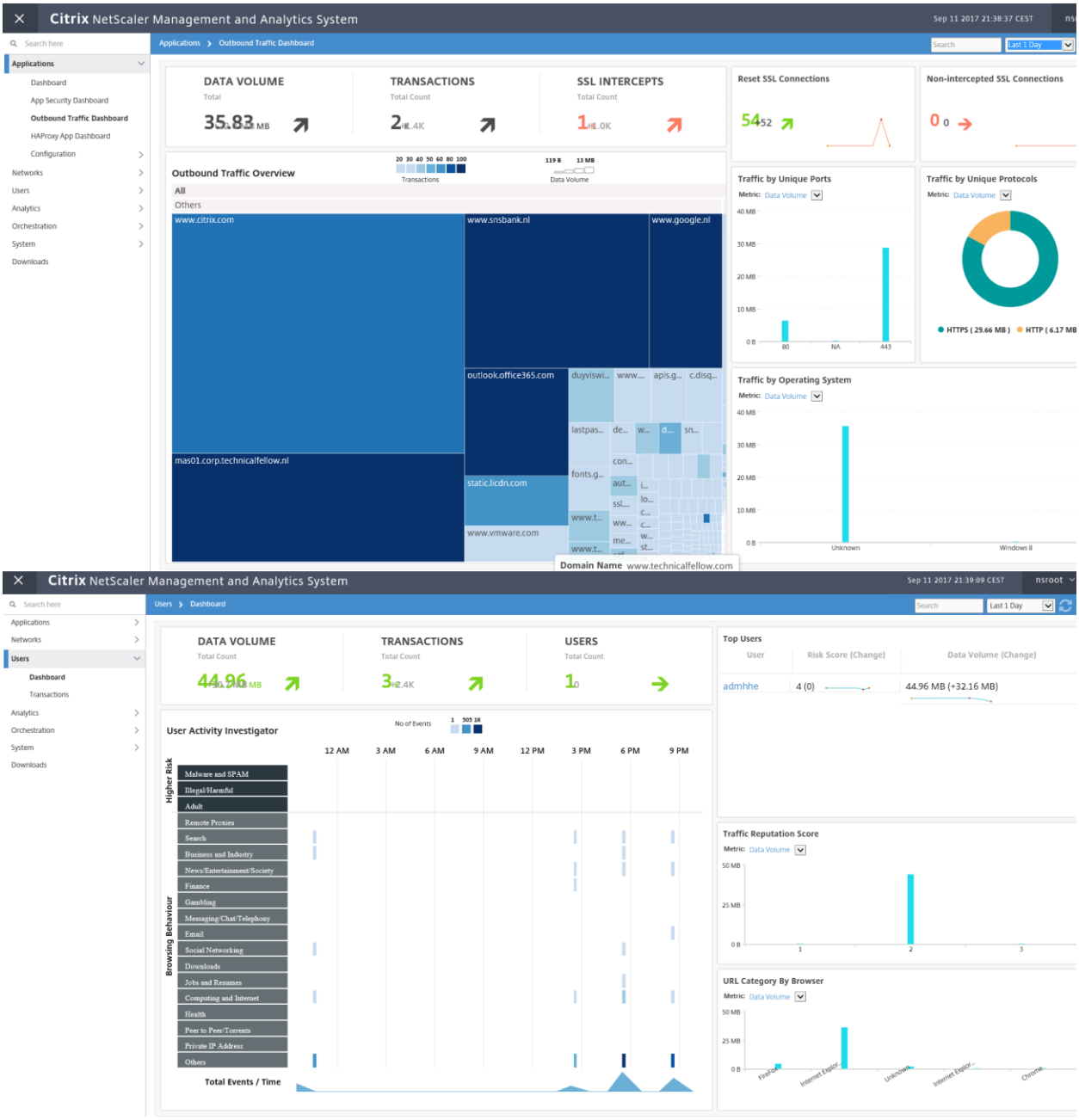
If you completed the article just as I did you will have an explicit proxy up and running, for simplicity I've also added a DNS record in my DNS zone for resolving the proxy VIP.

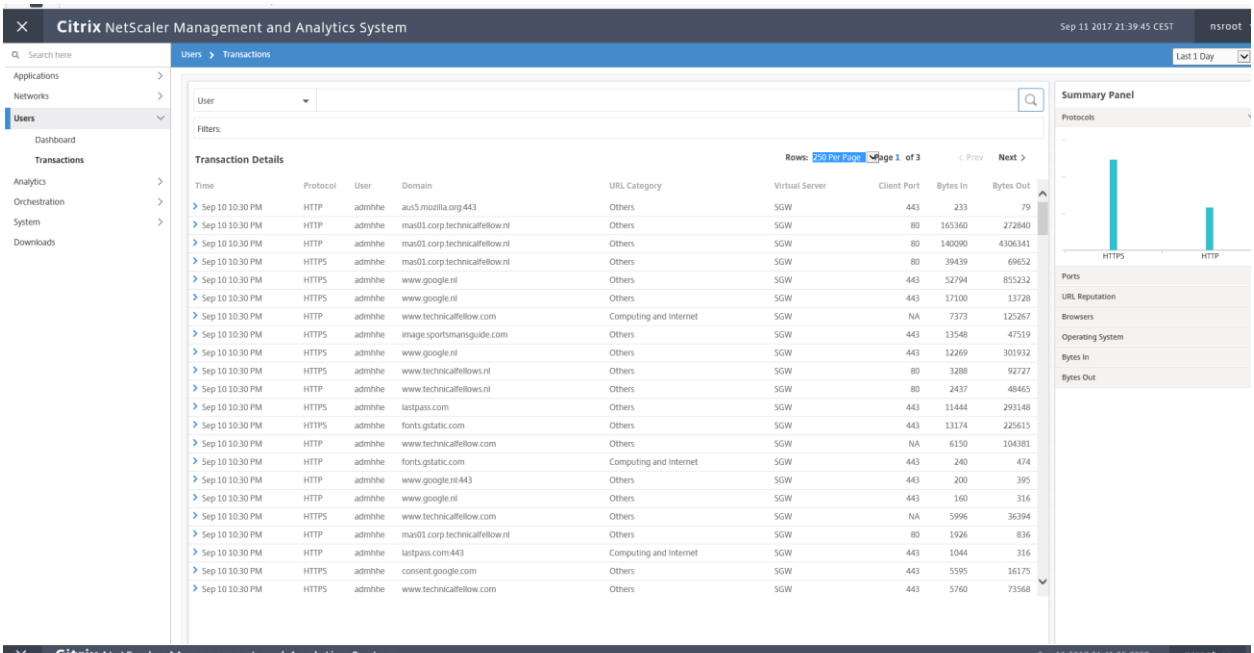


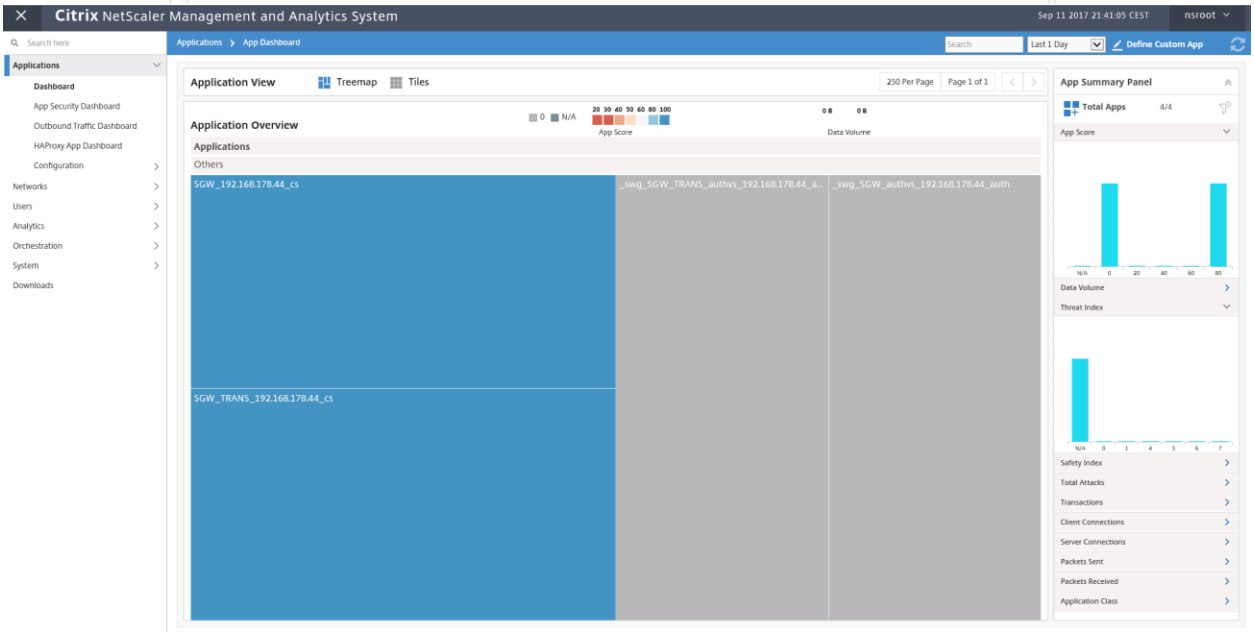
In addition you can also run the wizard again to create an transparent proxy, with all the same settings in place as the explicit one:

Regarding the configuration of Management and Analytics System (MAS) it's just adding the new VPX instance as a node in MAS an then data will show up as soon as you configured the proxy setup in your browser (explicit mode)

See the following screenshots for an overview:


Citrix NetScaler Management and Analytics System
Sep 11 2017 21:38:37 CEST
Applications › Outbound Traffic Dashboard
Search here
Applications
Dashboard
App Security Dashboard
Outbound Traffic Dashboard
HAProxy App Dashboard
Configuration
Networks
Users
Analytics
Orchestration
System
Downloads
DATA VOLUME
Total
TRANSACTIONS
Total Count
SSL INTERCEPTS
Total Count
Reset SSL Connections
Non-intercepted SSL Connections
Outbound Traffic Overview
Transactions
Data Volume
All
Others
www.citrix.com
www.snsbank.nl
www.google.nl
outlook.office365.com
mas01.corp.technicalfellow.nl
static.licdn.com
www.vmware.com
Traffic by Unique Ports
Traffic by Unique Protocols
HTTPS (29.66 MB)
HTTP (6.17 MB
Traffic by Operating System
Unknown
Windows 8
Domain Name www.technicalfellow.com
Citrix NetScaler Management and Analytics System
Sep 11 2017 21:39:09 CEST
nsroot
Users › Dashboard
Applications
Networks
Users
Dashboard
Transactions
Analytics
Orchestration
System
Downloads
DATA VOLUME
Total Count
TRANSACTIONS
Total Count
USERS
Total Count
Top Users
User
Risk Score (Change)
Data Volume (Change)
admhhe
4 (0)
44.96 MB (+32.16 MB)
User Activity Investigator
No of Events
12 AM
3 AM
6 AM
9 AM
12 PM
3 PM
6 PM
9 PM
Higher Risk
Browsing Behaviour
Malware and SPAM
Illegal/Harmful
Adult
Remote Proxies
Search
Business and Industry
News/Entertainment/Society
Finance
Gambling
Messaging/Chat/Telephony
Email
Social Networking
Downloads
Jobs and Resumes
Computing and Internet
Health
Peer to Peer/Torrents
Private IP Address
Others
Total Events / Time
Traffic Reputation Score
URL Category By Browser
Firefox
Internet Explor...
Unknown
Internet Explor...
Chrome


Citrix NetScaler Management and Analytics System
Sep 11 2017 21:39:45 CEST
nsroot
Search here
Applications
Networks
Users
Dashboard
Transactions
Analytics
Orchestration
System
Downloads
Users › Transactions
Last 1 Day
User
Filters:
Transaction Details
Rows: 250 Per Page Page 1 of 3
Prev
Next
Time Protocol User Domain URL Category Virtual Server Client Port Bytes In Bytes Out
Sep 10 10:30 PM HTTP admnhe aus5.mozilla.org:443 Others SGW 443 233 79
Sep 10 10:30 PM HTTP admnhe mas01.corp.technicalfellow.nl Others SGW 80 165360 272840
Sep 10 10:30 PM HTTP admnhe mas01.corp.technicalfellow.nl Others SGW 80 140090 4306341
Sep 10 10:30 PM HTTPS admnhe mas01.corp.technicalfellow.nl Others SGW 80 39439 69652
Sep 10 10:30 PM HTTPS admnhe www.google.nl Others SGW 443 52794 855232
Sep 10 10:30 PM HTTPS admnhe www.google.nl Others SGW 443 17100 13728
Sep 10 10:30 PM HTTP admnhe www.technicalfellow.com Computing and Internet SGW NA 7373 125267
Sep 10 10:30 PM HTTPS admnhe image.sportsmansguide.com Others SGW 443 13548 47519
Sep 10 10:30 PM HTTPS admnhe www.google.nl Others SGW 443 12269 301932
Sep 10 10:30 PM HTTPS admnhe www.technicalfellows.nl Others SGW 80 3288 92727
Sep 10 10:30 PM HTTP admnhe www.technicalfellows.nl Others SGW 80 2437 48465
Sep 10 10:30 PM HTTPS admnhe lastpass.com Others SGW 443 11444 293148
Sep 10 10:30 PM HTTPS admnhe fonts.gstatic.com Others SGW 443 13174 225615
Sep 10 10:30 PM HTTP admnhe www.technicalfellow.com Others SGW NA 6150 104381
Sep 10 10:30 PM HTTP admnhe fonts.gstatic.com Computing and Internet SGW 443 240 474
Sep 10 10:30 PM HTTP admnhe www.google.nl:443 Others SGW 443 200 395
Sep 10 10:30 PM HTTP admnhe www.google.nl Others SGW 443 160 316
Sep 10 10:30 PM HTTPS admnhe www.technicalfellow.com Others SGW NA 5996 36394
Sep 10 10:30 PM HTTP admnhe mas01.corp.technicalfellow.nl Others SGW 80 1926 836
Sep 10 10:30 PM HTTP admnhe lastpass.com:443 Computing and Internet SGW 443 1044 316
Sep 10 10:30 PM HTTPS admnhe consent.google.com Others SGW 443 5595 16175
Sep 10 10:30 PM HTTPS admnhe www.technicalfellow.com Others SGW 443 5760 73568
Summary Panel
Protocols
HTTPS
HTTP
Ports
URL Reputation
Browsers
Operating System
Bytes In
Bytes Out


Citrix NetScaler Management and Analytics System
Sep 11 2017 21:41:05 CEST
nsroot
Search here
Applications
Dashboard
App Security Dashboard
Outbound Traffic Dashboard
HAProxy App Dashboard
Configuration
Networks
Users
Analytics
Orchestration
System
Downloads
Applications › App Dashboard
Search
Last 1 Day
Define Custom App
Application View
Treemap
Tiles
250 Per Page
Page 1 of 1
Application Overview
0 N/A
20 30 40 50 60 80 100
App Score
Data Volume
Applications
Others
SGW_192.168.178.44_cs
_swg_SGW_TRANS_authvs_192.168.178.44_a...
_swg_SGW_authvs_192.168.178.44_auth
SGW_TRANS_192.168.178.44_cs
App Summary Panel
Total Apps 4/4
App Score
Data Volume
Threat Index
Safety Index
Total Attacks
Transactions
Client Connections
Server Connections
Packets Sent
Packets Received
Application Class