WHITE PAPER

A10 SSL INSIGHT & FIREWALL LOAD BALANCING WITH SONICWALL NEXT-GEN FIREWALLS

TABLE OF CONTENTS

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and non infringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

EXECUTIVE SUMMARY

This document describes how to implement SSL Deep Packet Inspection (DPI) inside a Firewall Load Balancing (FWLB) sandwich to improve availability, scalability and visibility across the IT infrastructure. The document focuses on SonicWall® SuperMassive next-generation firewalls for DPI, and A10 Networks Thunder SSL Insight® (SSLi®) for SSL decryption and FWLB.

INTRODUCTION

With the end-to-end security promised through SSL encryption, the threat of hidden attacks continues to increase, mandating organizations to decrypt and inspect SSL traffic. Organizations that do not decrypt and inspect traffic to unknown public sites create a blind spot that is left open for exploitation by data extrusion and malware, including advanced persistent threats (APTs). Most next-generation security devices are capable of decrypting SSL traffic and applying deep packet inspection policies. However, they are not designed specifically to handle the growing SSL traffic, coupled with increasing SSL key lengths and more computationally complex SSL ciphers. When facing a large volume of SSL traffic, most of the firewalls' resources get split between performing DPI and SSL decryption and re-encryption.

To enable business productivity, internet access must be operational and available at all times. This is sometimes referred to as "five nines" (99.999) uptime. Because things break, and unforeseen events do take place, organizations need to create an architecture that is highly available with failures predicted ahead of time, such that the only downtime is for planned maintenance.

A10 Networks SSL Insight technology provides a high-performance, highly available SSL decryption solution, which helps eliminate the SSL blind spot in corporate defenses and enables security devices to inspect encrypted traffic such as HTTPS, and not just clear text data in HTTP traffic.

SonicWall® SuperMassive firewalls provide high-performance DPI and threat protection along with centralized management and monitoring capabilities.

SOLUTION REQUIREMENTS

In order to achieve a robust SSL-DPI solution, the following requirements were set in place:

- High Availability:
  - Thunder SSLi appliances must be redundant
  - Individual SuperMassive firewalls must be redundant
  - Individual network links feeding into the system must be redundant
  - The FWLB sandwich should be resilient enough to preclude the need to take down the system for maintenance while upgrading a single firewall
- Scalability:
  - Capability to add more capacity as you continue reusing existing equipment
  - Support at least four SonicWall SuperMassive 9800 firewalls in the FWLB sandwich

- Throughput:
  - Support 40 Gbps of total throughput through the system
  - Demonstrate max SSL decryption capability using IXIA PerfectStorm cards
- Manageability:
  - Single point of management for all firewall clusters
  - Ability to enforce policies to multiple firewall cluster blades
- Design Constraints:
  - When the inside/decrypt zone fails over, the outside/re-encrypt zone must failover too
  - SuperMassive firewalls cannot communicate the above failover event from one zone to the other zone

SOLUTION COMPONENTS

In order meet the solution requirements, the following components were required:

- Four A10 Thunder 7440s with fully-loaded SSL security processors
- Four SonicWall SuperMassive 9800 firewalls operating in transparent mode
- Two Dell S6000 L3 switches
- A10 Networks Advanced Core Operating System (ACOS®) release 4.1.0-P5 or higher
- One 4x 10G LACP trunk (Port-Channel) ingress and one 4x 10G LACP trunk egress from the system
- One IXIA XGS12 Chassis with 4x 80G PerfectStorm cards

SOLUTION ARCHITECTURE

A10 Networks' SSL Insight solution consists of two processes:

- A decryption process, which operates on the secure/private side of an inline security device, takes encrypted traffic from the clients and decrypts it for the security device/s.
- A re-encryption process, which operates on the insecure/public side of an inline security device, takes traffic from the firewalls and re-encrypts it before sending it off to the internet gateway.

These decryption/re-encryption processes can both run on a single Thunder SSLi appliance, or they can be split out between two Thunder SSLi appliances, one dedicated for decryption, and the other for re-encryption. The primary advantage of the latter approach is increased performance (roughly 1.8x a single appliance) along with increased port density. Since our objective here was to achieve the maximum SSLi performance, we decided to use two Thunder SSLi appliances (one for decryption, one for re-encryption). Any inline security devices are sandwiched between these appliances as shown in Figure 1.

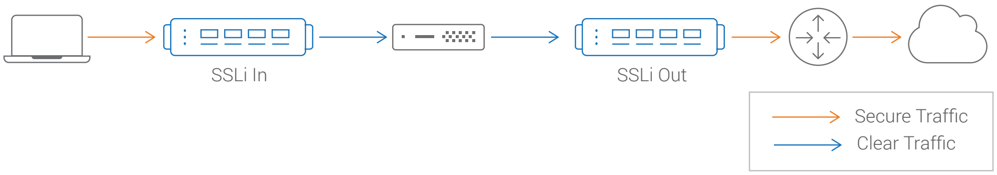


Figure 1: A10 Networks SSL Insight (SSLi) solution

The next step was achieving redundancy between the Thunder SSLi appliances. A10 Networks Thunder SSLi supports an Active-Standby HA deployment, whereby a VRRP based proprietary protocol, VRRP-a, is configured for monitoring failover decisions between the HA peers. In this case, it involved adding another pair of Thunder SSLi appliances to act as the Passive HA peers to the decryption as well as the re-encryption appliance.

The SonicWall SuperMassive firewalls were configured in transparent, bump-in-the-wire mode. Keeping the HA objective in perspective, each firewall had to be configured with two redundant paths, one between the Active Thunder SSLi appliances, the other between the Passive SSLi appliances. All four firewalls were connected in the same manner into a typical FWLB sandwich topology as shown in the Figure 2.

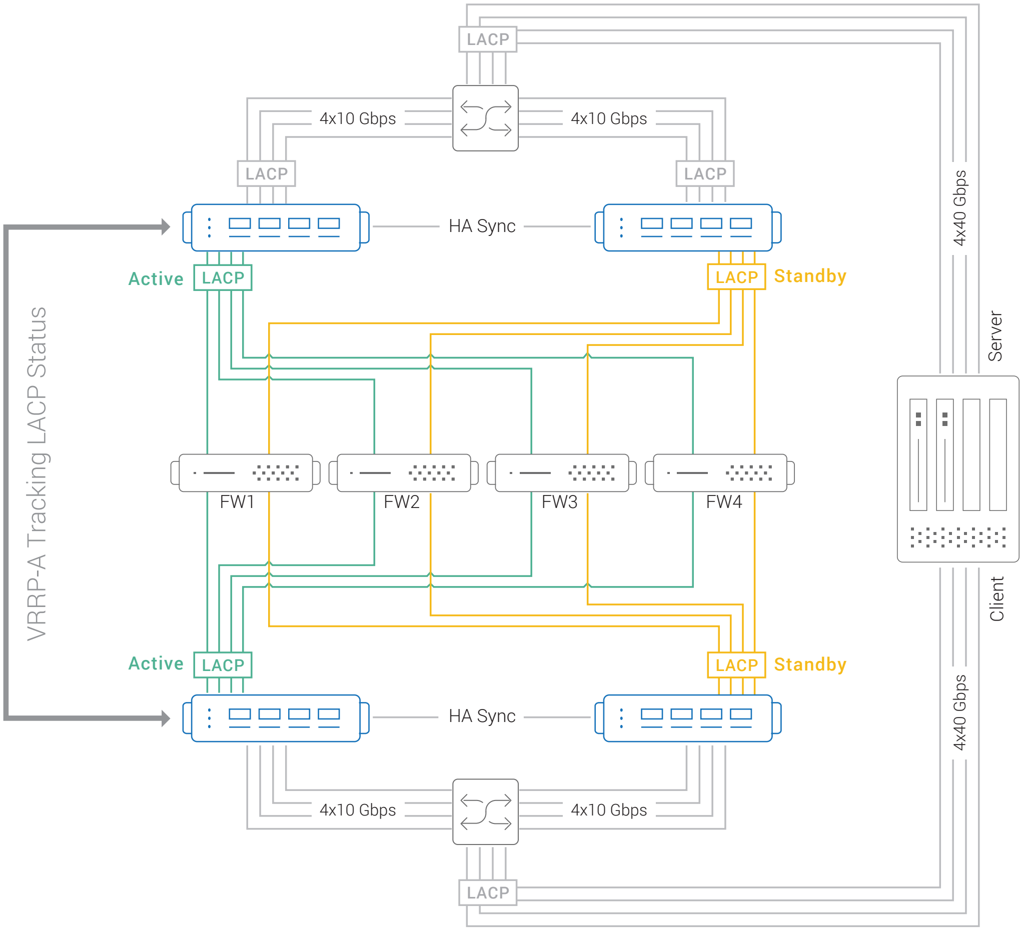


Figure 2: SSL Insight with firewall load balancing topology with Active-Standby HA

One of the design requirements was to perform a complete failover in the event that any device on the active path failed. For instance, if the active decryption Thunder SSLi appliance failed over, it should trigger the active re-encryption Thunder SSLi to also failover. Since it was not possible to communicate this failover through the firewalls, an alternate approach involving LACP trunking was used.

Using this method, essentially a single 4x10 Gbps port LACP trunk was configured between the decryption and the re-encryption Thunder SSLi appliances, with each SuperMassive firewall being a bump-in-the-wire on individual LACP member ports. This allowed the Thunder SSLi appliances to monitor both ends of the trunk and in the event that any trunk link went down, both Thunder SSLi appliances failed over to their HA peers, ensuring a complete failover.

The last piece was to ensure system resiliency, so if a single firewall got reloaded due to a software update etc. the system would not fail over, and traffic load would get redistributed to remaining active firewalls. This was achieved by tuning the LACP tracking configuration so the failover event was triggered only if more than one firewall failed. Using LACP as a FWLB mechanism was a design differentiator in this architecture, since it varied from the more standard method of using SLB and VRRP-a based configurations.

Lastly, the entire FWLB sandwich was connected between two Dell S6000 L3 switches using 4x10 Gbps port LACP trunks. Whereas the IXIA XGS12 chassis was connected so that 4x40 Gbps client traffic ports went to the inside Dell switch, the 4x40 Gbps server traffic ports went to the outside Dell switch as shown in the complete diagram in Figure 3.

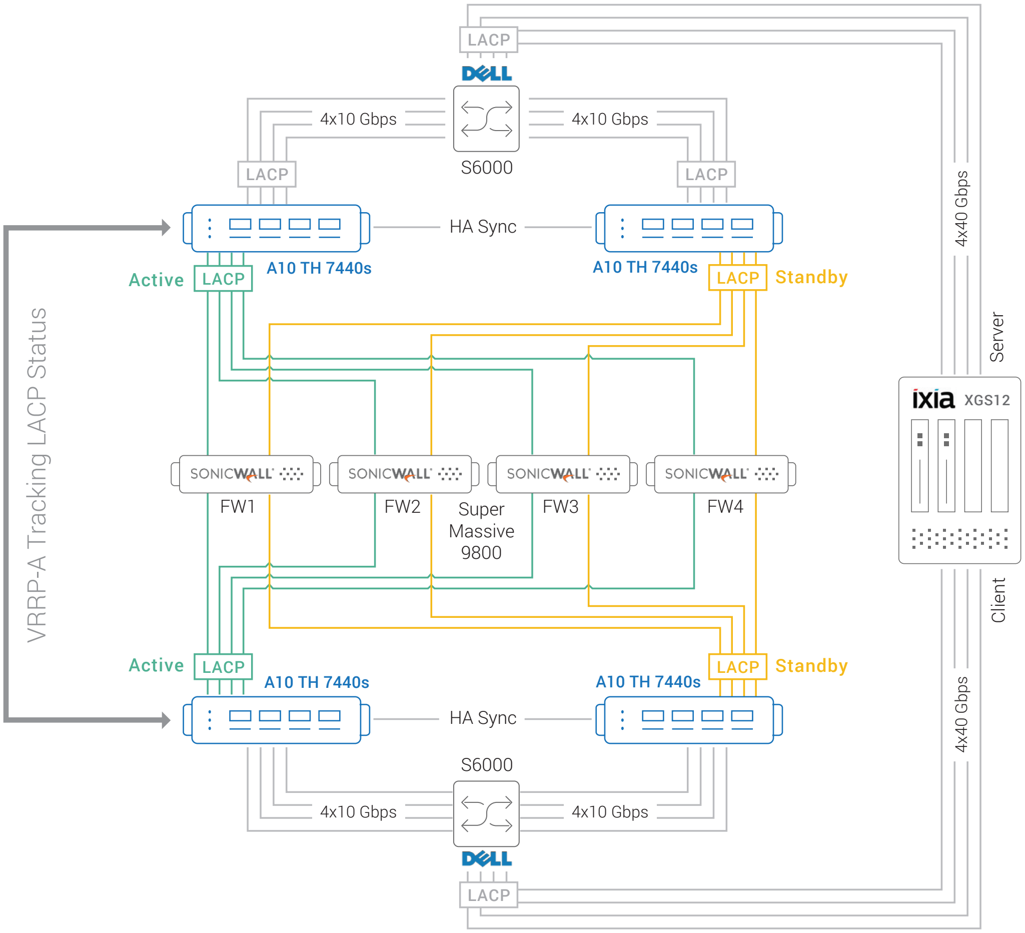


Figure 3: A10 Networks SSLi & firewall load balancing on SonicWall SuperMassive 9800 Firewalls

PERFORMANCE

The main criteria for the performance test was to achieve max SSLi throughput through the system. Since the physical bandwidth of the testbed capped at 40 Gbps, and we were able to achieve 40 Gbps of HTTP traffic with ease, IXIA IxLoad was configured to send up to 40 Gbps of SSL throughput traffic, using 4x40 Gbps PerfectStorm cards on the client side and 4x40 Gbps cards on the server side. The test objective was set to 'Throughput' and payload size was set to 1MB. We were able to achieve up to 30 Gbps of SSLi throughput with each Thunder SSLi running at about 75 percent CPUs, and about 35,000 concurrent connections.

Next, we added a constraint of maintaining 1 million concurrent connections at 30 Gbps. This was achieved with the following results:

Throughput:	30 Gbps**
Connections per second:	5,000
Concurrent Connections:	1 million
Thunder SSLi CPUs:	90 percent

We also triggered multiple failovers during the course of this test and verified minimal failover times with full system recovery.

*** A10 Networks can scale beyond 4x inline SonicWall SuperMassive firewalls to up to 8x inline firewalls. However, the SSLi throughput is capped at 75 Gbps with the most advanced Thunder SSLi appliances.*

CONFIGURATIONS

The following configurations were used for this solution.

CONFIGURATION ON A10 THUNDER SSLI APPLIANCES

ACTIVE-DECRYPT

```
!64-bit Advanced Core OS (ACOS) version 4.1.0-
P5, build 135
(Aug-30-2016,22:08)

!

!multi-ctrl-cpu 8

!

vrrp-a common

  device-id 1

  set-id 1

  enable

!

access-list 101 permit ip any any

!

vlan 100

  untagged trunk 1

  router-interface ve 100

!

vlan 200

  untagged trunk 2

  router-interface ve 200

!

vlan 999

  untagged trunk 3

  router-interface ve 999

!

hostname Int-SSLi

!

interface management

  ip address 192.168.1.114 255.255.255.0

  ip default-gateway 192.168.1.1

!

interface ethernet 1

  trunk-group 1 lacp

    timeout short

!
```

STANDBY-DECRYPT

```
!64-bit Advanced Core OS (ACOS) version 4.1.0-
P5, build 135
(Aug-30-2016,22:08)

!

!multi-ctrl-cpu 8

!

vrrp-a common

  device-id 2

  set-id 1

  enable

!

access-list 101 permit ip any any

!

vlan 100

  untagged trunk 1

  router-interface ve 100

!

vlan 200

  untagged trunk 2

  router-interface ve 200

!

vlan 999

  untagged trunk 3

  router-interface ve 999

!

hostname Int-SSLi

!

interface management

  ip address 192.168.1.112 255.255.255.0

  ip default-gateway 192.168.1.1

!

interface ethernet 1

  trunk-group 1 lacp

    timeout short

!
```

ACTIVE-DECRYPT

```
interface ethernet 2
  trunk-group 1 lacp
    timeout short
!
interface ethernet 3
  trunk-group 1 lacp
    timeout short
!
interface ethernet 4
  trunk-group 1 lacp
    timeout short
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
interface ethernet 18
  trunk-group 2 lacp
    timeout short
!
interface ethernet 19
  trunk-group 3
!
interface ethernet 20
  trunk-group 2 lacp
    timeout short
!
interface ethernet 21
  trunk-group 3
!
interface ethernet 22
  trunk-group 2 lacp
    timeout short
!
```

STANDBY-DECRYPT

```
interface ethernet 2
  trunk-group 1 lacp
    timeout short
!
interface ethernet 3
  trunk-group 1 lacp
    timeout short
!
interface ethernet 4
  trunk-group 1 lacp
    timeout short
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
interface ethernet 18
  trunk-group 2 lacp
    timeout short
!
interface ethernet 19
  trunk-group 3
!
interface ethernet 20
  trunk-group 2 lacp
    timeout short
!
interface ethernet 21
  trunk-group 3
!
interface ethernet 22
  trunk-group 2 lacp
    timeout short
!
```

ACTIVE-DECRYPT

```
interface trunk 2
  ports-threshold 3 timer 1 do-auto-recovery
!
interface ve 100
  ip address 10.0.0.1 255.255.0.0
  ip allow-promiscuous-vip
!
interface ve 200
  ip address 20.0.0.1 255.255.255.0
!
interface ve 999
  ip address 99.9.0.1 255.255.255.0
!
vrrp-a vrid 0
  floating-ip 10.0.0.10
  floating-ip 20.0.0.10
  blade-parameters
    priority 200
    tracking-options
      trunk 3 priority-cost 60
!
vrrp-a preferred-session-sync-port trunk 3
!
ip route 0.0.0.0 /0 20.0.0.11
!
slb template port default
  health-check-disable
!
slb template server default
  health-check-disable
!
slb template tcp-proxy tcp
  receive-buffer 50000000
  transmit-buffer 50000000
!
slb template tcp-proxy timeout
  idle-timeout 120
  half-close-idle-timeout 60
!
```

STANDBY-DECRYPT

```
interface trunk 2
  ports-threshold 3 timer 1 do-auto-recovery
!
interface ve 100
  ip address 10.0.0.2 255.255.0.0
  ip allow-promiscuous-vip
!
interface ve 200
  ip address 20.0.0.2 255.255.255.0
!
interface ve 999
  ip address 99.9.0.2 255.255.255.0
!
vrrp-a vrid 0
  floating-ip 10.0.0.10
  floating-ip 20.0.0.10
  blade-parameters
    tracking-options
      trunk 3 priority-cost 60
!

vrrp-a preferred-session-sync-port trunk 3
!
ip route 0.0.0.0 /0 20.0.0.11
!
slb template port default
  health-check-disable
!
slb template server default
  health-check-disable
!
slb template tcp-proxy tcp
  receive-buffer 50000000
  transmit-buffer 50000000
!
slb template tcp-proxy timeout
  idle-timeout 120
  half-close-idle-timeout 60
!
```

ACTIVE-DECRYPT

```
slb server fw1 20.0.0.11
  port 0 tcp
  port 0 udp
  port 8080 tcp
!
slb service-group sg1-8080 tcp
  member fw1 8080
!
slb service-group sg1-tcp tcp
  member fw1 0
!
slb service-group sg1-udp udp
  member fw1 0
!
slb template client-ssl c-ssl
  forward-proxy-ca-cert a10-BPcert
  forward-proxy-ca-key a10-BPkey
  forward-proxy-ocsp-disable
  forward-proxy-crl-disable
  forward-proxy-enable
!
slb virtual-server vip1 0.0.0.0 acl 101
  port 0 tcp
    service-group sg1-tcp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 443 https
    service-group sg1-8080
    use-rcv-hop-for-resp
    template client-ssl c-ssl
    template tcp-proxy tcp
    no-dest-nat port-translation
!
end
```

STANDBY-DECRYPT

```
slb server fw1 20.0.0.11
  port 0 tcp
  port 0 udp
  port 8080 tcp
!
slb service-group sg1-8080 tcp
  member fw1 8080
!
slb service-group sg1-tcp tcp
  member fw1 0
!
slb service-group sg1-udp udp
  member fw1 0
!
slb template client-ssl c-ssl
  forward-proxy-ca-cert A10-BP.cert
  forward-proxy-ca-key A10-BP.cert
  forward-proxy-ocsp-disable
  forward-proxy-crl-disable
  forward-proxy-enable
!
slb virtual-server vip1 0.0.0.0 acl 101
  port 0 tcp
    service-group sg1-tcp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 443 https
    service-group sg1-8080
    use-rcv-hop-for-resp
    template client-ssl c-ssl
    template tcp-proxy tcp
    no-dest-nat port-translation
!
end
```

ACTIVE-DECRYPT

```
!64-bit Advanced Core OS (ACOS) version 4.1.0-P5, build 135 (Aug-30-2016,20:48)
!
!multi-ctrl-cpu 8
!
vrrp-a common
  device-id 1
  set-id 2
  enable
!
access-list 101 permit ip any any vlan 200
!
vlan 200
  untagged trunk 2
  router-interface ve 200
!
vlan 300
  untagged trunk 1
  router-interface ve 300
vlan 999
  untagged trunk 3
  router-interface ve 999
!
hostname Ext-SSLi
!
interface management
  ip address 192.168.1.115 255.255.255.0
  ip default-gateway 192.168.1.1
!
interface ethernet 1
  trunk-group 1 lacp
    timeout short
!
interface ethernet 2
  trunk-group 1 lacp
    timeout short
!
interface ethernet 3
  trunk-group 1 lacp
    timeout short
!
interface ethernet 4
  trunk-group 1 lacp
    timeout short
!
```

STANDBY-DECRYPT

```
!64-bit Advanced Core OS (ACOS) version 4.1.0-P5, build 135 (Aug-30-2016,20:48)
!
!multi-ctrl-cpu 8
!
vrrp-a common
  device-id 2
  set-id 2
  enable
!
access-list 101 permit ip any any vlan 200
!
vlan 200
  untagged trunk 2
  router-interface ve 200
!
vlan 300
  untagged trunk 1
  router-interface ve 300
vlan 999
  untagged trunk 3
  router-interface ve 999
!
hostname Ext-SSLi
!
interface management
  ip address 192.168.1.113 255.255.255.0
  ip default-gateway 192.168.1.1
!
interface ethernet 1
  trunk-group 1 lacp
    timeout short
!
interface ethernet 2
  trunk-group 1 lacp
    timeout short
!
interface ethernet 3
  trunk-group 1 lacp
    timeout short
!
interface ethernet 4
  trunk-group 1 lacp
    timeout short
!
```

ACTIVE-DECRYPT

```
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
interface ethernet 18
  trunk-group 2 lacp
    timeout short
!
interface ethernet 19
  trunk-group 3
!
interface ethernet 20
  trunk-group 2 lacp
    timeout short
!
interface ethernet 21
  trunk-group 3
!
interface ethernet 22
  trunk-group 2 lacp
    timeout short
!
interface trunk 2
  ports-threshold 3 timer 1 do-auto-recovery
!
interface ve 200
  ip address 20.0.0.3 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 300
  ip address 30.0.0.3 255.255.0.0
!
interface ve 999
  ip address 99.9.1.3 255.255.255.0
```

STANDBY-DECRYPT

```
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
interface ethernet 18
  trunk-group 2 lacp
    timeout short
!
interface ethernet 19
  trunk-group 3
!
interface ethernet 20
  trunk-group 2 lacp
    timeout short
!
interface ethernet 21
  trunk-group 3
!
interface ethernet 22
  trunk-group 2 lacp
    timeout short
!
interface trunk 2
  ports-threshold 3 timer 1 do-auto-recovery
!
interface ve 200
  ip address 20.0.0.4 255.255.255.0
  ip allow-promiscuous-vip
!
interface ve 300
  ip address 30.0.0.4 255.255.0.0
!
interface ve 999
  ip address 99.9.1.4 255.255.255.0
```

ACTIVE-DECRYPT

```
vrrp-a vrid 0
  floating-ip 30.0.0.11
  floating-ip 20.0.0.11
  blade-parameters
    priority 200
    tracking-options
      trunk 3 priority-cost 60
!
vrrp-a preferred-session-sync-port trunk 3
!
ip route 0.0.0.0 /0 30.0.0.20
ip route 10.0.0.0 /16 20.0.0.10
!
slb template port default
  health-check-disable
!
slb template server-ssl s-ssl
  forward-proxy-enable
!
slb template tcp-proxy tcp
  receive-buffer 50000000
  transmit-buffer 50000000
!
slb server DG 30.0.0.20
  port 0 tcp
  port 0 udp
  port 443 tcp
!
slb service-group sg1-443 tcp
  member DG 443
!
slb service-group sg1-tcp tcp
  member DG 0
!
slb service-group sg1-udp udp
  member DG 0
!
```

STANDBY-DECRYPT

```
vrrp-a vrid 0
  floating-ip 30.0.0.11
  floating-ip 20.0.0.11
  blade-parameters
    tracking-options
      trunk 3 priority-cost 60
!

vrrp-a preferred-session-sync-port trunk 3
!
ip route 0.0.0.0 /0 30.0.0.20
ip route 10.0.0.0 /16 20.0.0.10
!
slb template port default
  health-check-disable
!
slb template server-ssl s-ssl
  forward-proxy-enable
!
slb template tcp-proxy tcp
  receive-buffer 50000000
  transmit-buffer 50000000
!
slb server DG 30.0.0.20
  port 0 tcp
  port 0 udp
  port 443 tcp
!
slb service-group sg1-443 tcp
  member DG 443
!
slb service-group sg1-tcp tcp
  member DG 0
!
slb service-group sg1-udp udp
  member DG 0
!
```

ACTIVE-DECRYPT

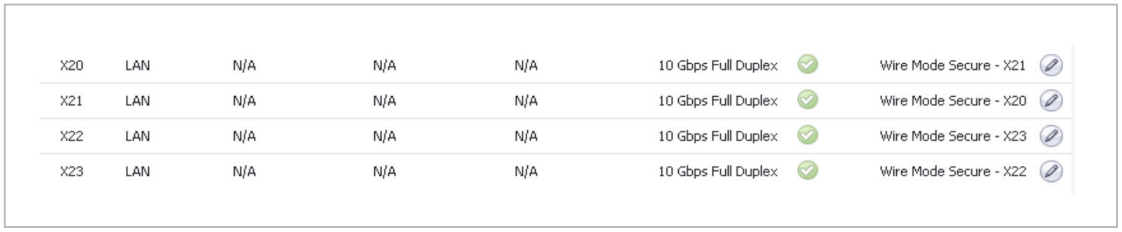
```
slb virtual-server vip1 0.0.0.0 acl 101
  port 0 tcp
    service-group sg1-tcp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 8080 http
    service-group sg1-443
    use-rcv-hop-for-resp
    template server-ssl s-ssl
    template tcp-proxy tcp
    no-dest-nat port-translation
!
end
```

STANDBY-DECRYPT

```
slb virtual-server vip1 0.0.0.0 acl 101
  port 0 tcp
    service-group sg1-tcp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 udp
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 0 others
    service-group sg1-udp
    use-rcv-hop-for-resp
    no-dest-nat
  port 8080 http
    service-group sg1-443
    use-rcv-hop-for-resp
    template server-ssl s-ssl
    template tcp-proxy tcp
    no-dest-nat port-translation
!
end
```

CONFIGURATION ON SONICWALL SUPERMASSIVE FIREWALLS

The SonicWall Next Generation Firewalls used in our validation are SuperMassive 9800s. Each firewall is fully licensed and configured in wire secure mode as follows:



X20	LAN	N/A	N/A	N/A	10 Gbps Full Duplex	✓	Wire Mode Secure - X21	✎
X21	LAN	N/A	N/A	N/A	10 Gbps Full Duplex	✓	Wire Mode Secure - X20	✎
X22	LAN	N/A	N/A	N/A	10 Gbps Full Duplex	✓	Wire Mode Secure - X23	✎
X23	LAN	N/A	N/A	N/A	10 Gbps Full Duplex	✓	Wire Mode Secure - X22	✎

For security services, Intrusion Prevention service is enabled and configured to detect and prevent all attacks. All other configurations are standard default configuration.

Please refer to SonicWall documentation for further details.

CONCLUSION

A10 Networks Thunder SSLi has been successfully deployed with SonicWall SuperMassive Next-Gen firewalls in a fully redundant Firewall Load Balancing sandwich. All solution requirements were met at the design level and we also achieved our performance objective of 30 Gbps of SSLi throughput at 1 million concurrent connections.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.com/contact

Part Number: A10-WP-21149-EN-01 JAN 2018