DEPLOYMENT GUIDE

A10 SSL INSIGHT & SONICWALL NEXT-GEN FIREWALLS

A10 NETWORKS SSL INSIGHT & FIREWALL LOAD BALANCING SOLUTION FOR SONICWALL SUPERMASSIVE NEXT GENERATION FIREWALLS

OVERVIEW

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. This guide focuses on SonicWALL™ SuperMassive Next Generation Firewalls for DPI, and A10 Networks® Thunder SSL Insight® (SSLi®) for SSL decryption and FWLB.

TALK
WITH A10

CONTACT US
a10networks.com/contact

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 noninfringement. 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.

DEPLOYMENT REQUIREMENTS

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

- 4x A10 Thunder 7440s with fully-loaded SSL security processors
- 4x on SonicWALL SuperMassive 9800 firewalls operating in Transparent mode
- 2x Dell S6000 L3 switches
- A10 Networks Advanced Core Operating System (ACOS®) release 4.1.0-P5 or higher
- 4x10G LACP trunks (Port-Channels) in and out the system
- 1x IXIA XGS12 Chassis with 4x 80G PerfectStorm cards

To achieve a robust SSL-DPI solution, we have set the following requirements:

- High-Availability (HA):
  - 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 such that there is no need to take down system for maintenance while upgrading a single firewall
- Scalability:
  - Capability to add more capacity as you continue reusing existing equipment
  - Support at least 4x on 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 the firewall cluster, 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

ACCESSING A10 THUNDER SSLI

Thunder SSLi can be accessed either from a Command Line Interface (CLI) or a Graphical User Interface (GUI). For this deployment, we are using the CLI for the configuration of the Thunder SSLi devices:

CLI

This is a text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or the network via SSHv2. The system default values are:

Default username: admin

Default password: a10

Default IP address of the device: 172.31.31.31

> ***Note**: Thunder SSLi can also be configured using the standard GUI that can be accessed by entering the management IP address in a web browser's address bar (e.g., https://172.31.31.31) and using the default access credentials mentioned above.*

> ***Note**: The first configuration to consider is to change the management IP address for CLI and GUI access. If you are using two separate devices to deploy SSL Insight, make sure that both systems are configured with a separate management IP address.*

THE A10 NETWORKS SSL INSIGHT AND SONICWALL SUPERMASSIVE NGFW COMBINED SOLUTION

A10 Networks SSL Insight solution consists of two processes:

- A decryption process which operates on the secure/private side of an inline security device that takes encrypted traffic from the clients and decrypts it for the security device/s.
- A re-encryption process which operates on the unsecured/public side of an inline security device that 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 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 single

appliance) along with increased port density. The objective here is to achieve the maximum SSLi performance, therefore we will 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.

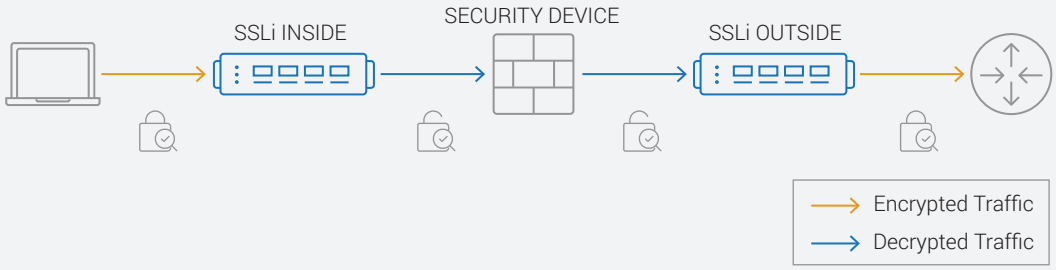

Figure 1: A10 Networks SSL Insight (SSLi) solution

The next step is achieving redundancy between Thunder SSLi appliances. A10 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 deployment, another pair of Thunder SSLi appliances is added to act as the Passive HA peers to the decryption, as well as the re-encryption appliance.

Figure 2 shows a typical HA deployment of SSLi with multiple active firewalls. Here, the firewalls are deployed in transparent, bump-in-the-wire mode. Keeping HA objectives in perspective, each firewall is configured with two redundant paths, one between the Active Thunder SSLi appliances, and the other between the Passive Thunder SSLi appliances.

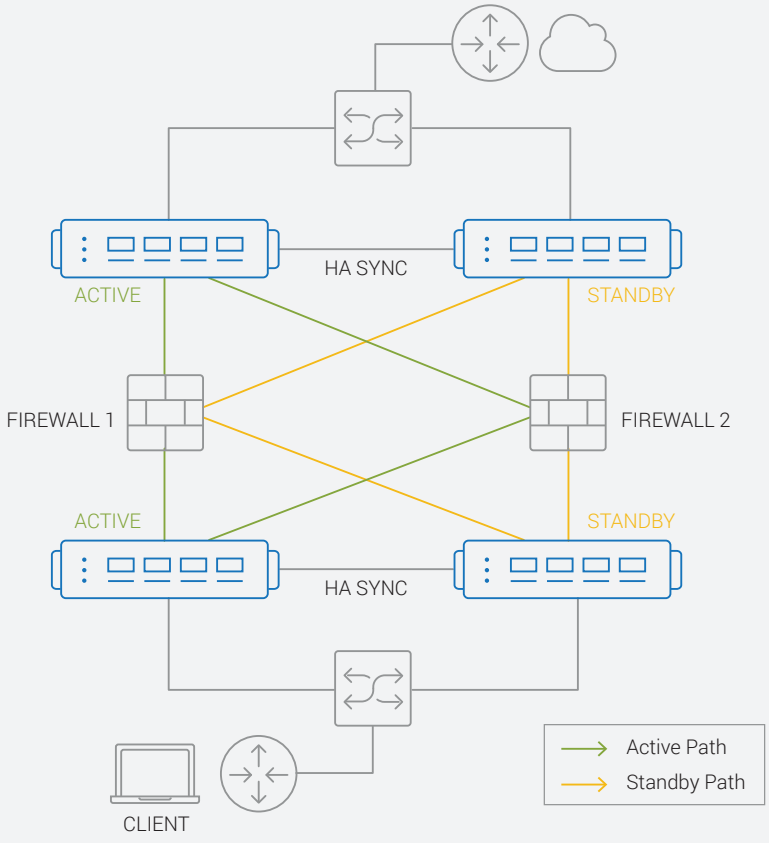

Figure 2: SSL Insight with firewall load balancing topology with Active-Standby HA

For this specific deployment use case, the design requirement is to perform a complete failover in the event that any device on the active path fails. 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 is not possible to communicate this failover through the firewalls, an alternate approach, involving Link Aggregation Control Protocol (LACP) trunking is used. Using this method, a single 4x10 Gbps port LACP trunk is configured between the decryption and the re-encryption Thunder SSLi appliances, with each SuperMassive firewall serving as a bump-in-the-wire on individual LACP member ports. This allows 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.

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

Lastly, the entire FWLB sandwich is connected in between two Dell S6000 L3 switches using 4x10 Gbps port LACP trunks. The IXIA XGS12 chassis is both as a Client and a Server, and is connected so that 4x40 Gbps client traffic ports are connected to the inside Dell switch, and 4x40 Gbps server traffic ports are connected to the outside Dell switch as shown in the complete diagram in Figure 3.

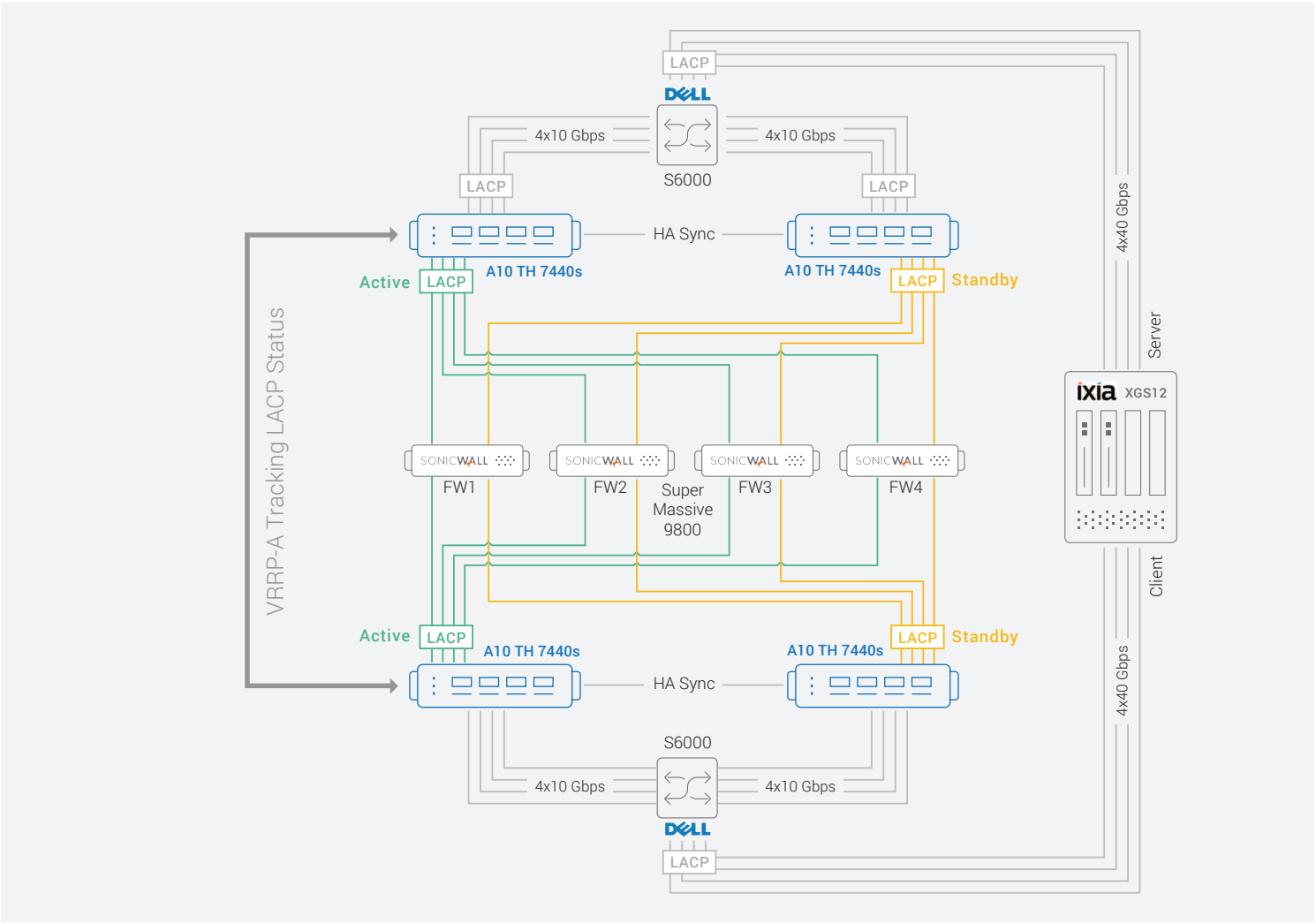

Figure 3: A10 Networks SSLi & Firewall Load balancing of on SonicWALL SuperMassive 9800 Firewalls

***Note**: For detailed configuration files, refer to the Appendices.*

PERFORMANCE

The main criteria for the performance test is to achieve max SSLi throughput through the system. Since the physical bandwidth of the testbed caps at 40 Gbps, and we are able to achieve 40 Gbps of HTTP traffic with

ease; IXIA IxLoad is 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 is set to 'throughput' and payload size is set to 1 MB.

With the above configuration, SSLi throughput of up to 30 Gbps can be achieved, with each Thunder SSLi appliance running at about 75% CPUs, and about 35,000 concurrent connections.

A constraint of maintaining 1 million concurrent connections at 30 Gbps is set, which is achieved with the following results:

Throughput: 30 Gbps

Connections per second: 5,000

Concurrent Connections: 1M

Thunder SSLi CPUs: 90%

For testing purposes, multiple failover events were triggered to verify minimal failover times with full system recovery.

APPENDIX A

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
```

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 192.168.1.114 255.255.255.0
  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
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
interface ethernet 18
```

```
  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
!
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
!
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
!
```

```
  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 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
!
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
```

```
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
!
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-ReEncrypt

```
!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
!
```

```
!
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- ReEncrypt

```
!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 192.168.1.115 255.255.255.0
  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
!
interface ethernet 15
  trunk-group 3
!
interface ethernet 16
  trunk-group 2 lacp
    timeout short
!
interface ethernet 17
  trunk-group 3
!
```

```
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
!
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
!
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
!
```

```
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
!
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
!
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
```

```
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
!
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
```

```
    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
```

APPENDIX B

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 following:

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.

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

©2018 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-DG-16166-EN-02 FEB 2018