TECH NOTE

SECURE WAN ACCELERATION IMPLEMENTATION GUIDE

CISCO WAAS AND CISCO ASA/PIX (VER. 7.2.3)

The Cisco ASA/PIX release version 7.2.3 introduces an enhancement to enable a security-compliant WAN optimization solution using the Cisco Wide Area Application Services Software. This solution provides full stateful inspection capabilities, facilitates Payment Card Industry (PCI) compliance, transparently protects WAN accelerated traffic, and provides transparent integration for networks using Cisco WAAS. This document describes the configuration required for deploying Cisco Wide Area Application Services (WAAS) with the Cisco ASA/PIX version 7.2.3 or later.

OVERVIEW

Cisco WAAS provides an automatic discovery mechanism that uses TCP options during the initial three-way handshake to identify Cisco WAE appliances transparently. After automatic discovery, optimized connections experience a shift in the TCP sequence number to allow endpoints to distinguish between optimized and non-optimized flows. Cisco ASA/PIX release starting at 7.2.3 has incorporated an enhancement to permit the sequence number jump initiated by Cisco WAAS without compromising stateful inspection of TCP flows. Internal firewall TCP state variables are adjusted to take into account the presence of the Cisco WAE Appliances, and as a result, stateful Layer 4 inspection is performed on Cisco WAAS optimized TCP sessions. Other ASA/PIX functionalities, such as VPN and NAT are also supported for optimized connections. We continue to supported Layer 7 inspection for non-optimized traffic.

SOLUTION DETAILS

An enhancement in Cisco ASA/PIX Release 7.2.3 or later allows the ASA/PIX to recognize traffic being optimized by Cisco WAAS. With this enhancement, the Cisco ASA/PIX observes the TCP options used in WAAS automatic discovery. When the Cisco ASA/PIX notices that a connection has successfully completed WAAS automatic discovery, it permits the initial sequence number shift for the connection and maintains the Layer 4 state on the optimized path.

CLI Command: To allow Cisco ASA/PIX Firewall to recognize, permit and secure Cisco WAAS optimized traffic, a new command-line interface (CLI) is provided. The new CLI should be enabled as part of the class Modular Policy Framework (MPF) to facilitate Cisco ASA/PIX Firewall interoperability with Cisco WAAS. The CLI command is as follows:

```
policy-map global_policy
 class inspection_default
   inspect waas
```

Configuration details are provided in the Appendix at the end of this document. This solution details section provides implementation guidance while highlighting the steps to be taken into consideration when deploying a WAAS with ASA/PIX. In order for the ASA/PIX to understand WAAS connection, “inspect waas” CLI was added to the policy-map. For standard TCP based applications such as HTTP, WAAS traffic will be recognized by the ASA/PIX during the WAE auto-discovery process, and WAAS optimization will work seamlessly while the ASA/PIX keeps the state of the TCP flow. The traffic will be marked with “W” flag on the ASA/PIX.

```
ciscoasa# show conn detail
14 in use, 24 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, O - outbound data,
       P - inside back connection, q - SQL*Net data, R - outside acknowledged FIN,
```

```
      R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
      s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, W - WAAS,
      X - inspected by service module
TCP outside:17.14.100.31/80 inside:10.10.10.31/10000 flags UOW
```

Additionally, when a WAAS connection is confirmed, the following informational message will be printed in syslog.

```
ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port,
inspection services bypassed on this connection.
```

Note: WAEs use port 443 and 8443 to communicate with the Central Manager and for GUI access. In addition, if CIFS acceleration is configured, port 4050 is used for the WAFS connection directive. These ports need to be allowed on firewalls or router ACLs.

Dynamic Application Port Negotiation

Some applications use a control channel to dynamically negotiate a port number to be used for data transfer. For these protocols, the ASA/PIX creates pinholes for the data channel dynamically as the port number is negotiated. FTP, H323, SIP, and SCCP (Skinny) are examples of some of the applications that use dynamic application port negotiation. For most of these applications, the default policy on WAE is to pass-through the control channel traffic as these types of traffic receive limited benefit from WAAS. As a result, the ASA/PIX can observe the port negotiated and open pinholes for these applications to function as usual. For example, with FTP, the control channel (port 21) payload is passed through by WAAS. As a result, the ASA/PIX can observe the port negotiation and open ports for the data channel of the FTP file transfer.

Some protocols use the same port for control and data, such as RTSP, SUNRPC and SQL*Net, the default policy in WAAS is Full Optimization. When deploying with the ASA/PIX, the policy for these applications in WAAS needs to be changed to Pass Through. This is required so that the ASA/PIX can "see" the un-compressed payload from the primary (control) channel to get the port number negotiated for the secondary (data) channel, and therefore allow the secondary channel to establish.

NAT Configuration for CIFS Optimization

CIFS traffic (port 139 and 445) is intercepted by the edge WAE and goes through a pre-established WAFS transport channel (port 4050) between the core and edge WAEs. When CIFS traffic comes out from the WAFS transport channel on the server side WAE, it has passed the firewall, with a NATed destination IP address of the server. The NATed server IP address is not known on the INSIDE. Please follow the steps below to ensure the server can be discovered by the core WAE with its real IP address, and for successful CIFS acceleration. A sample configuration is provided in the Appendix section.

- On the data center router, configure NAT to make the translation between the global (outside) IP address and the real (inside) IP address of the server.
- Configure WCCP interception for service groups 61 and 62 on the WAN interface of the router. This is to insure NAT works correctly on the server side.

IPS and CSC Module

ASA Firewalls have the capability of providing Intrusion Protection Services and content security protection services via the use of the Advanced Inspection and Prevention Security Services Module (AIP-SSM), and the Content Security and Control Security Services Module (CSC-SSM).

With the AIP-SSM module installed and configured, once WAAS auto-discovery is confirmed, i.e. option 33 is observed during the TCP 3-way handshake, the AIP-SSM inspection will be by-passed. All TCP based applications will be optimized by WAAS according to the configured policy.

The CSC-SSM module proxies TCP connections and thus will disable WAAS optimization. **The CSC-SSM module is not supported with WAAS deployment.**

IPSec VPN

When site-to-site IPSec VPNs are deployed between the Branch and Data Center ASA/PIX, the MSS usually needs to be adjusted to account for the GRE tunnel and/or encryption protocol overhead. The TCP payload will be checked for WAAS-optimized connections to insure it is within MSS advertised by the peer. In WAAS versions prior to 4.0.13, we use a static MSS of 1432 for optimized connections. WAAS version 4.0.13 has a new feature to automatically adjust MSS, thus no additional configuration is required. If WAAS version prior to 4.0.13 is used, it is necessary to either:

1) change the optimized-mss to something <= the MSS advertised by the client/server, or 2) disable the MSS check in ASA.

Please refer to the whitepaper "WAAS interaction with TCP MSS" on the Sales Rack (http://wwwin-tools.cisco.com/sales/servlet/getDocument?message_id=450563&linkurl=/salesrack/products/sw/contnetw/ps6870&portalID=35517) for more information on adjusting MSS value.

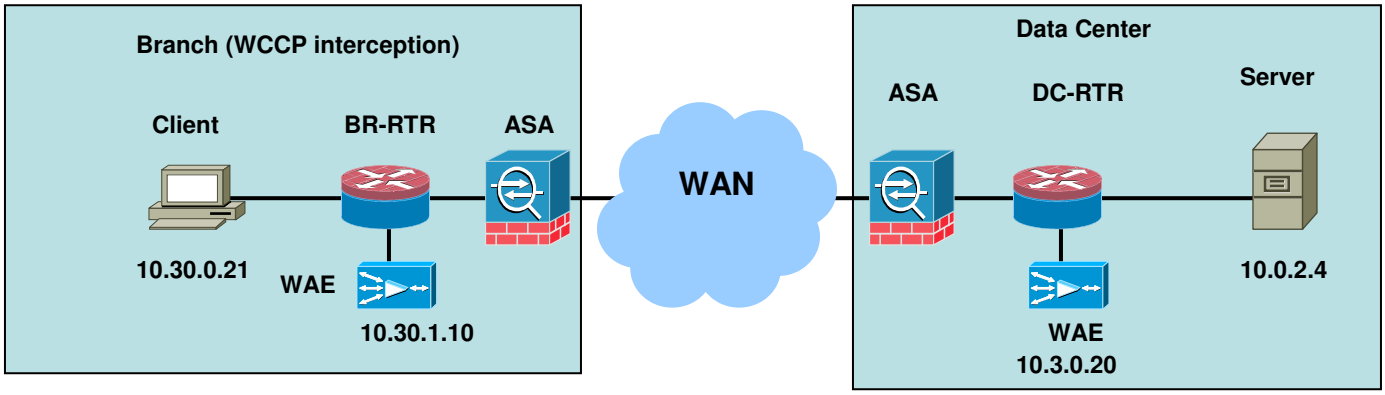
DEPLOYMENT SCENARIOS:

WAAS with ASA/PIX

Figure 1 below shows a baseline deployment scenario with the WAEs implemented at the branch and the data center using WCCP protocol for interception and redirection. Configuration of the Branch side ASA in this configuration is provided in the Appendix.

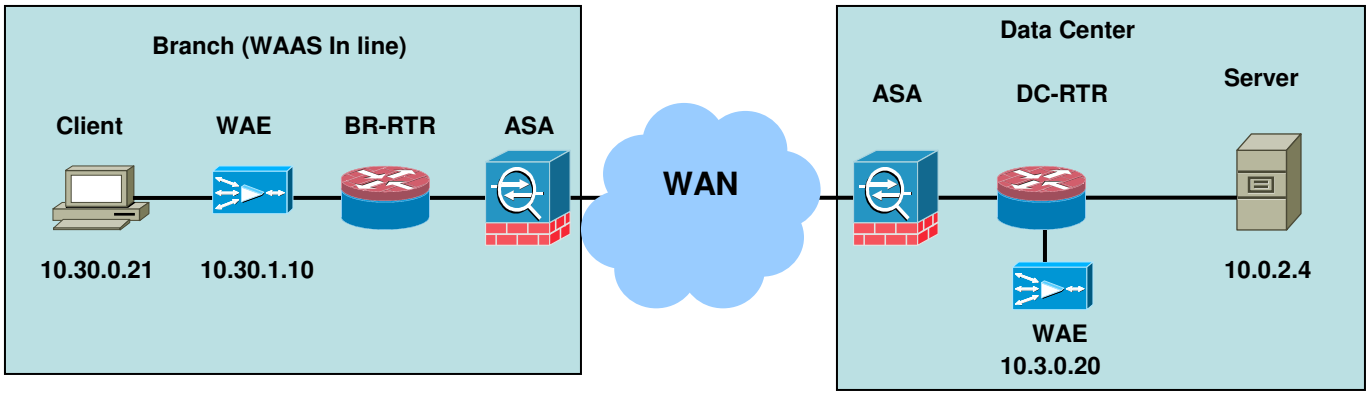
Note: WCCP interception needs to be configured on routers with a supported IOS version**. Please do not configure WCCP redirection on the ASA/PIX as it is not a supported configuration.**

Figure 1: WAAS appliance with ASA deployment with WCCP interception at the Branch



In a Branch office, a WAE appliance can also be deployed as an inline device. This deployment is supported and the ASA at the branch can share the same configuration as in the above scenario. Figure 2 below depicts a deployment with the Branch WAE implemented using inline interception.

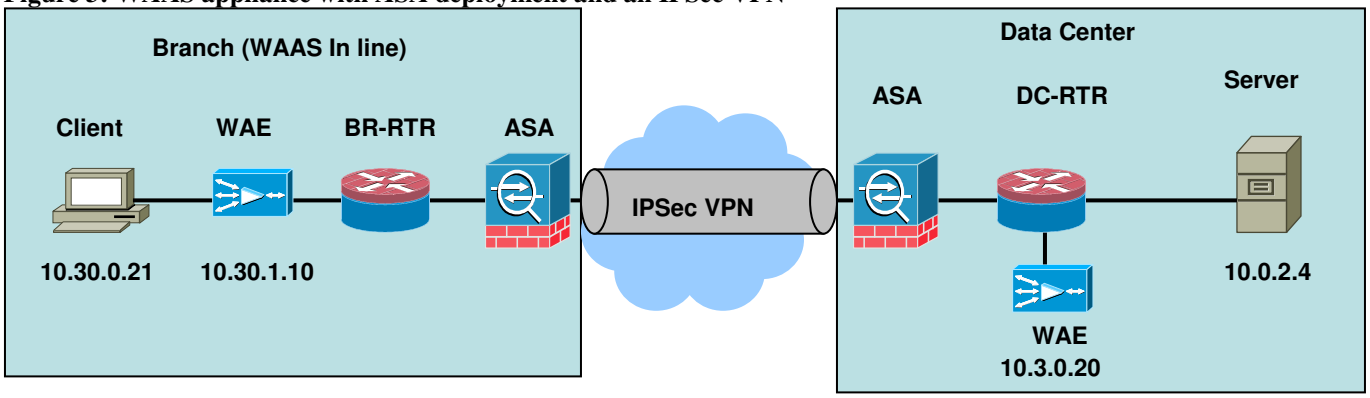
Figure 2: WAAS appliance with ASA deployment with inline interception at the Branch



WAAS with IPSec and ASA/PIX

In addition to the baseline deployment, having an IPSec VPN between the ASA/PIX Firewalls is a common deployment scenario. A sample configuration is provided in the Appendix.

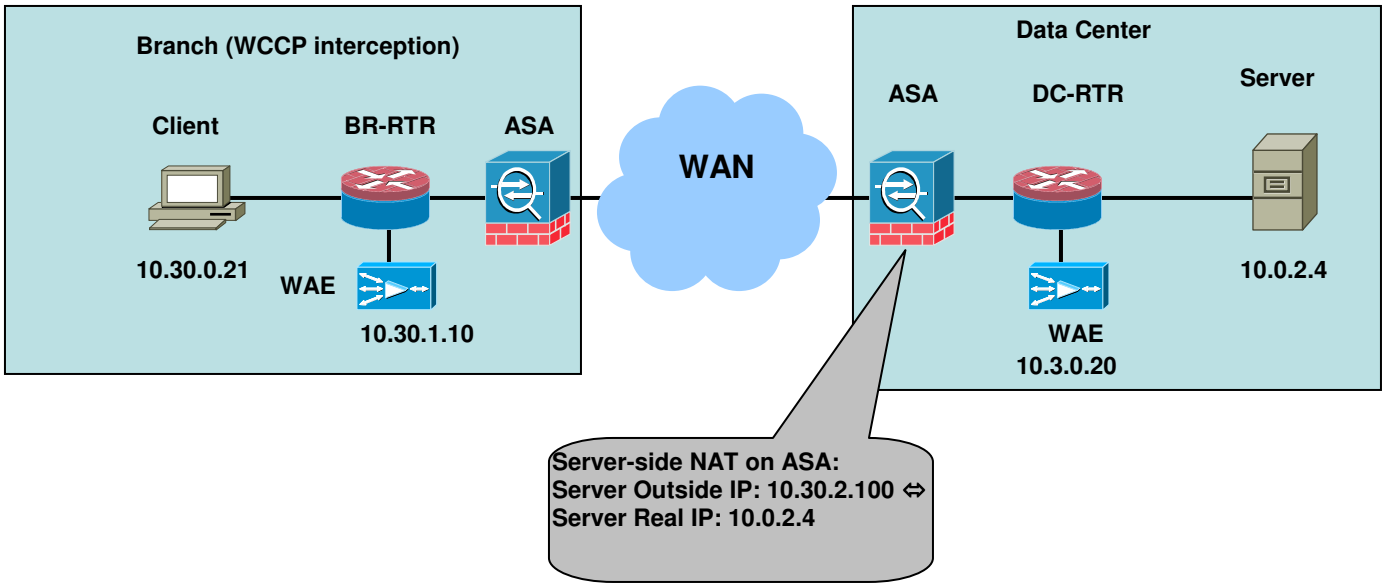
Figure 3: WAAS appliance with ASA deployment and an IPSec VPN



WAAS with NAT and ASA/PIX

NAT configuration is commonly used on ASA/PIX Firewalls. Both client-side and server-side NAT are supported. When client-side NAT is configured and inline interception is used for the branch WAE, client-side NAT works seamlessly with no special configurations required. When Server-side NAT is configured, and WCCP interception is used on the data center side, TCP optimization (TFO/DRE/LZ) works seamlessly. In order for CIFS auto-discovery to work properly, additional steps need to be taken as described in the Solution Details section of this document. A sample configuration is provided in the Appendix.

Figure 4: WAAS appliance with ASA deployment with Server-side NAT



CONCLUSION

The Cisco ASA/PIX Firewall Software Release version 7.2.3 or later includes an enhancement to enable a security-compliant WAN optimization and application acceleration solution using Cisco WAAS. With this enhancement, the integration of WAAS and ASA is transparent, and the Firewall maintains layer 4 inspection capability, while also maintaining state on all Cisco WAAS optimized TCP sessions. An IPSec VPN deployed between two ASA/PIX units is also supported with WAAS implementation.

APPENDIX

Baseline ASA Configuration

```
waas-branch# sh run
: Saved
:
ASA Version 7.2(2)33
!
hostname waas-branch
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.30.3.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.30.2.3 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
```

```
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 171.68.96.120 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa722-33-k8.bin
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
same-security-traffic permit intra-interface
access-list outside_access_in extended permit tcp 10.3.0.0 255.255.255.0 any eq https ← Allows
WAAS management port
access-list outside_access_in extended permit tcp 10.3.0.0 255.255.255.0 any eq 8443 ← Allows
WAAS management port
access-list outside_access_in extended permit tcp 10.3.0.0 255.255.255.0 any eq 4050 ← Allows
WAAS management port
access-list outside_access_in extended permit tcp 10.3.0.0 255.255.255.0 any eq www ← Allows WAAS
management port
access-list outside_access_in extended permit tcp host 10.0.2.4 any eq 8443 ← Needed to access the
branch WAE GUI
access-list inside_access_in extended permit ip any any
pager lines 24
logging enable
logging console debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
access-group inside_access_in in interface inside
access-group outside_access_in in interface outside
route inside 10.30.0.0 255.255.255.0 10.30.3.1 1
route inside 10.30.1.0 255.255.255.0 10.30.3.1 1
route outside 10.0.2.0 255.255.254.0 10.30.2.1 1
route outside 10.0.254.0 255.255.254.0 10.30.2.1 1
route outside 10.3.0.0 255.255.255.0 10.30.2.1 1
route outside 10.30.4.0 255.255.255.0 10.30.2.1 1
route management 0.0.0.0 0.0.0.0 171.68.96.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 management
telnet timeout 180
ssh scopy enable
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum 512
policy-map global_policy
  class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect waas
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:c11b71317b49a3b461a8a3d7c19e47d1
: end
```

ASA + VPN

Branch ASA

```
access-list outside_cryptomap_2 extended permit ip any any

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 2 match address outside_cryptomap_2
crypto map outside_map 2 set pfs
crypto map outside_map 2 set peer 10.30.2.1
crypto map outside_map 2 set transform-set ESP-3DES-SHA
crypto map outside_map 2 set nat-t-disable
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

tunnel-group 10.30.2.1 type ipsec-l2l
tunnel-group 10.30.2.1 ipsec-attributes
 pre-shared-key *
```

Data Center ASA

```
access-list outside_20_cryptomap extended permit ip any any

crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 10.30.2.3
crypto map outside_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map 20 set nat-t-disable
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400

tunnel-group 10.30.2.3 type ipsec-l2l
```

```
tunnel-group 10.30.2.3 ipsec-attributes
 pre-shared-key *
```

ASA + Client Side NAT

```
global (outside) 1 10.30.2.100
nat (inside) 1 10.30.0.0 255.255.255.0
nat (outside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 10.30.1.10 10.30.1.10 netmask 255.255.255.255
```

ASA + Server Side NAT

```
static (inside,outside) 10.30.2.100 10.0.2.4 netmask 255.255.255.255
```

Router Configuration with Server Side NAT

```
interface FastEthernet0/0.30
 description Pod3 DC LAN
 encapsulation dot1Q 30
 ip address 10.3.0.1 255.255.255.0
 ip wccp redirect exclude in
 ip nat outside
 no snmp trap link-status
!
interface FastEthernet0/0.254
 encapsulation dot1Q 254
 ip address 10.0.254.30 255.255.255.0
 ip nat inside
 no snmp trap link-status


interface FastEthernet0/1
 description WAN interface
 ip address 10.30.4.2 255.255.255.0
 ip wccp 61 redirect out
 ip wccp 62 redirect in
 duplex full
 speed 100
ip nat inside source static 10.0.2.4 10.30.2.100
```

WAE Configuration

WAE configuration is not supplied here as standard configuration can be applied. No special configuration is required,